



KUNGL
TEKNISKA
HÖGSKOLAN



HØGSKOLEN
I GJØVIK

NISlab

Norwegian Information
Security Laboratory

Is BS 7799 worth the effort?

Frank-Arne Stamland



Institutionen för
Data- och Systemvetenskap

Examensarbete
Nr 2004-x-164
2002

Examensarbete 20 poäng
i data- och systemvetenskap
inom magisterprogrammet i informations- och kommunikations säkerhet,
Kungl Tekniska Högskolan



KUNGL
TEKNISKA
HÖGSKOLAN



HØGSKOLEN
I GJØVIK

NISlab

Norwegian Information
Security Laboratory

Is BS 7799 worth the effort?

Frank-Arne Stamland



Institutionen för
Data- och Systemvetenskap

Examensarbete
Nr 2004-x-164
2002

Examensarbete 20 poäng
i data- och systemvetenskap
inom magisterprogrammet i informations- och kommunikations säkerhet,
Kungl Tekniska Högskolan

Preface

It is a pleasure to finish my master thesis and I look forward to new targets within information security (IS). Completing this master thesis has been a very valuable process for me.

This master thesis is written in connection with my master study in information security at Gjøvik University College, Norway. The master programme is a co-operation between Gjøvik University College and KTH, the Royal Institute of Technology in Sweden.

I wish to give thanks to my supervisor Professor Einar Snekkenes for his contribution to this master thesis. I also wish to give thanks to all my student colleagues, the staff at Gjøvik University College and the staff at KTH.

I also wish to thank my employer VincIT AS which have supported the master study both financially and by releasing me from work. VincIT AS is at this time one of the nine organisations in Norway which are certified according to BS 7799-2:2002.

One of the reasons for choosing BS 7799 as a subject is that I have been using BS 7799 since 1996 in many IS projects. I have also been involved in a number of BS 7799 certification schemes. In these years I have often been met by the comments "What's the point of using time on BS 7799 certification or even BS 7799 at all?" The master thesis report is my contribution to showing the effects of using BS 7799 for implementing an Information Security Management System (ISMS). We believe that the ISMS will act as a foundation for getting the grips with the IS challenge in most organisations.

Porsgrunn, June 30, 2004
Frank-Arne Stamland

frank-arne.stamland@vincit.no

Abstract

This thesis will focus on whether organisations which have certified their ISMS according to BS 7799 achieve a better capability for preventing, detecting, and reacting to security breaches, so that the consequences of security breaches may be reduced. The thesis will also explore if there is any difference between organisations which use the BS 7799 informally versus organisations which do not use the standard at all.

In these days, it is a challenge for the information community that IS is managed in many different ways. Today, and in the future, it may be vital that IS is handled according to a set of common principles independent of the organisation.

We conducted a survey in the form of a questionnaire. The questionnaire was distributed to IS manager or IS staff in 40 Norwegian organisations which we expected to have implemented a type of ISMS. Eight of the organisations were certified according to BS 7799-2 and we had a clear expectation that a focus on IS was an important issue in the remaining organisations.

In the questionnaire we asked the organisations for the following:

- the consequences of security breaches which have hit the organisations from 1999 to 2004, estimated as financial loss
- how security breaches are handled in the organisation and the possibilities for us to get access to statistical data regarding security breaches
- which parts of the ISMS are implemented and how they are implemented

In regard to the questions about ISMS, we asked about the vital parts which should have been implemented in all organisations which have a certain need for protecting their assets.

The replies regarding the consequences of and the statistical data on security breaches were too few to compare certified organisations, organisations using the standard informal and organisations not using a standard at all.

The rest of the questionnaire focused on the vital parts of the ISMS. The replies to these questions made it possible to estimate the maturity level of the ISMS within the organisations. The ISMS maturity level may be regarded as a reflection of the IS status of the organisations.

The conclusions in this thesis are that organisations certified according to BS 7799-2 have a higher maturity level versus organisations which have chosen to implement an ISMS informally. Those organisations which have implemented an informal ISMS have higher maturity than those organisations which have not implemented an ISMS at all.

Sammendrag

Denne masteroppgaven fokuserer på hvorvidt organisasjoner som har sertifisert sitt styringssystem for informasjonssikkerhet etter BS 7799, oppnår en bedre evne til å forebygge, detektere og reagere på sikkerhetsbrudd slik at konsekvensene ved sikkerhetsbrudd reduseres. Masteroppgaven vil også utforske om det er en forskjell på organisasjoner som benytter BS 7799 på en uformell måte kontra organisasjoner som ikke benytter standarden.

I disse dager er det en utfordring for informasjonssamfunnet at informasjonssikkerhet et styrt og håndtert på mange forskjellige måter. I dag, og i fremtiden, kan det være vitalt å kunne håndtere informasjonssikkerheten iht. et felles sett med prinsipper, uavhengig av organisasjon.

Vi har gjennomført en undersøkelse i form av en spørreundersøkelse. Spørreundersøkelsen ble distribuert til sikkerhetssjefer eller stabspersonell innen informasjonssikkerhet i 40 norsk virksomheter hvor vi forventet at et styringssystem for informasjonssikkerhet var implementert. Åtte av virksomhetene var sertifisert etter BS 7799-2. Vi hadde også klare forventninger til at informasjonssikkerhet var et viktig tema i de andre virksomhetene.

I spørreundersøkelsen spurte vi organisasjonene om følgende:

- konsekvensene som har rammet organisasjonen fra 1999 til 2004, estimert som økonomiske tap
- hvordan brudd på informasjonssikkerhet er håndtert i organisasjonen og mulighetene for oss til å få tilgang til de statistiske data angående brudd på sikkerheten
- hvilke deler av styringssystemer som er implementert og hvordan det er implementert

Angående spørsmålet om styringssystem for informasjonssikkerhet spurte vi om de vitale delene som burde vært implementert i alle virksomheter med et visst behov for å beskytte organisasjonens verdier.

Svarene angående konsekvenser og statistiske data angående brudd på sikkerheten var for få til å sammenligne sertifiserte organisasjoner, organisasjoner som benytter standarden uformelt og de organisasjoner som ikke benytter en standard.

Resten av spørreskjemaet fokuserte på de vitale delene av et styringssystem for informasjonssikkerhet. Svarene på disse spørsmålene gjorde det mulig å estimere modenhetsnivået på organisasjonens styringssystem for informasjonssikkerhet. Modenhetsnivået på styringssystemet for informasjonssikkerhet kan ansees som et speilbilde av nivået på informasjonssikkerheten i organisasjonene.

Konklusjonene i denne masteroppgaven er at sertifiserte organisasjoner har et høyere modenhetsnivå enn organisasjoner som har valgt å benytte standarden til å implementere et uformelt styringssystem for informasjonssikkerhet. De organisasjoner som har implementert et uformelt styringssystem har et høyere modenhetsnivå enn de organisasjonene som ikke har implementert noen form for styringssystem.

Table of contents

PREFACE.....	II
ABSTRACT	III
SAMMENDRAG	IV
TABLE OF CONTENTS.....	V
TABLE OF FIGURES.....	VII
TABLE OF TABLES.....	VII
1. INTRODUCTION.....	1
1.1 TOPIC.....	1
1.2 RESEARCH PROBLEM.....	1
1.3 MOTIVATION/SIGNIFICANCE	1
1.4 RESEARCH QUESTIONS	2
1.5 SEARCHING FOR LITERATURE	3
2. BACKGROUND AND THEORY	4
2.1 RELATED WORK AND STATE OF THE ART	4
2.1.1 <i>Information and definition about the problem that the BS 7799 standard shall solve</i>	<i>4</i>
2.1.2 <i>How many organisations are certified according to BS 7799-2?</i>	<i>5</i>
2.1.3 <i>What kinds of organisations are certified according to BS 7799?.....</i>	<i>5</i>
2.1.4 <i>To what extent have organisations using BS 7799 solved the problem?</i>	<i>5</i>
2.2 BS 7799 AND INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)	7
2.3 THE MATURITY MODEL	10
2.3.1 <i>More about the five levels of software process maturity</i>	<i>13</i>
2.3.2 <i>COBIT and Management Guidelines</i>	<i>15</i>
2.3.3 <i>Maturity of information risk management.....</i>	<i>16</i>
2.4 SECURITY METRICS GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS	18
3. SURVEY.....	20
3.1 CHOICE OF METHOD	20
3.1.1 <i>Mix method approach</i>	<i>21</i>
3.1.2 <i>Validity and reliability of the method chosen</i>	<i>22</i>
3.2 QUESTIONNAIRE	23
3.2.1 <i>Gained experience from pilot survey.....</i>	<i>23</i>
3.2.2 <i>Selection of organisations from private sector and public sector</i>	<i>23</i>
3.2.3 <i>The questionnaire</i>	<i>24</i>
3.3 CARRYING OUT THE SURVEY	24
4. RESULTS.....	25
4.1 GENERAL INFORMATION AND STATISTIC FROM THE SURVEY	25
4.1.1 <i>The main activity in the participating organisation.....</i>	<i>25</i>
4.1.2 <i>Distribution regarding the number of employees.....</i>	<i>26</i>
4.2 THE DISTRIBUTION OF ISMS IN USE	26
4.3 IS RESOURCES IN USE AND RESOURCES IN USE ON PREVENTIVE MEASURES.....	27
4.4 IS POLICY IN THE ORGANISATIONS	28
4.5 MANAGEMENT FORUM FOR IS	28
4.6 AWARENESS	28
4.7 RISK ANALYSIS.....	28
4.8 BUSINESS CONTINUITY MANAGEMENT	29
4.9 IS BREACHES AND STATISTICS IN THE ORGANISATIONS	31
4.10 HANDLING SECURITY BREACHES - INCIDENT RESPONSE TEAM	32
4.11 CONSEQUENCES IN THE ORGANISATIONS.....	33

4.12	DETERMINATION OF THE ORGANISATIONS ISMS MATURITY LEVEL	34
4.13	STATISTICAL ESTIMATES	36
4.13.1	<i>Bootstrap - estimation of average for certified organisations</i>	36
4.13.2	<i>Bootstrap - estimation of average for informal use of the standard</i>	37
4.13.3	<i>Bootstrap - estimation of average for organisations that do not use any standard</i>	38
4.13.4	<i>Boxplot</i>	39
5.	DISCUSSION	40
5.1	PRACTICAL PROBLEMS	42
6.	CONCLUSION AND FURTHER WORK.....	43
6.1	FURTHER WORK.....	43
7.	REFERENCES	45
APPENDIX A: ACCOMPANYING LETTER DISTRIBUTED WITH THE QUESTIONNAIRE.....		1
APPENDIX B: LETTER OF RECOMMENDATION FROM THE NORWEGIAN MINISTRY OF TRADE AND INDUSTRY.....		2
APPENDIX C: QUESTIONNAIRE		4
APPENDIX D: THE ANSWERS FROM THE QUESTIONNAIRE		9
APPENDIX E: THE QUESTIONNAIRE TRANSLATED INTO ENGLISH WITH AN EXPLANATION AND INTENTIONS.....		17
APPENDIX F: BOOTSTRAP PROGRAM AND THE PROGRAM RESULTS		25

Table of figures

Figure 1: Systematized security concepts [1]	8
Figure 2: The risk management model [1]	9
Figure 3: PDCS model applied to ISMS processes [4]	10
Figure 4: The Capability Maturity Model for Software [6].....	11
Figure 5: The five levels of software process maturity [18].....	13
Figure 6: A management view of visibility into the software process at each maturity level [18].....	14
Figure 7: Process Maturity Model scoring from 0 to 5 [9].....	15
Figure 8: Main activity in the participating organisations.....	25
Figure 9: The number of employees in the organisations	26
Figure 10: The distribution of ISMS.....	26
Figure 11: IS resources in use.....	27
Figure 12: IS resources in use on preventive measures as a percent of the total resources in use.....	27
Figure 13: IS Awareness campaigns and training.....	28
Figure 14: When is risk analysis carried out?.....	29
Figure 15: Business continuity management in the organisations	30
Figure 16: Question 25i, testing frequency	31
Figure 17: Question 25l, updating frequency	31
Figure 18: Statistical register regarding security breaches	32
Figure 19: Handling security breaches in the organisations	32
Figure 20: Actual consequences experienced by the organisations	33
Figure 21: The actual consequences estimated as financial loss	34
Figure 22: Maturity level for certified organisations	36
Figure 23: Maturity level for the informal use of the standard.....	37
Figure 24: Maturity level for organisations which do not use any standard	38
Figure 25: An overall shape of the bootstrap data	39

Table of tables

Table 1: Maturity of information risk management [1, 26].....	16
Table 2: The classification of certification in the ISMS [1]	18
Table 3: The international ISMS standards in risk management cycle [1]	18
Table 4: Which elements is a part of the business continuity management process?	30
Table 5: Statistics for security breaches in the organisations, retrospective in years	32
Table 6: Team to handle security breaches - numbered years in existence	33
Table 7: The organisations ISMS maturity level	35
Table 8: Number of organisations within each type of ISMS and maturity level	35
Table 9: The mean maturity level of the organisations within each type of ISMS.....	41

1. Introduction

1.1 Topic

The topic in this master thesis is to show whether organisations using BS 7799 in a formal or informal way achieve a better capability for preventing, detecting, and reacting to security breaches, so that the consequences of security breaches may be reduced.

The origin of BS 7799 and ISO/IEC 17799 (ISO/IEC: International Organisation for Standardization and International Electrotechnical Commission) goes back to the days of the UK Department of Trade and Industry's (DTI) Commercial Computer Security Centre (CCSC). Founded in May 1987, the CCSC had two major tasks. The first was to help vendors of IT security products by establishing a set of internationally recognised security evaluation criteria and an associated evaluation and certification scheme. This ultimately gave rise to the ITSEC and the establishment of the UK ITSEC Scheme. The second task was to help users by producing a code of good security practice resulting in a "User's Code of Practice" published in 1989 [14].

Since then, further developments and versions of the standards have been made. Current versions are:

- ISO/IEC 17799 which is used as a code of best practice for Information Security (IS). This guideline is issued by ISO/IEC [13].
- BS 7799 part 2 is the specification used in the certification scheme [4].

BS 7799 [4] can be used by internal and external parties, including certification bodies, to assess an organisation's ability to meet its own requirements, as well as any customer demands or regulatory demands. The goal of this thesis is to show whether international standards for IS, in the context as formal certification schemes, correspond to expectations.

1.2 Research problem

Many organisations find it difficult and costly to handle the IS in a proper way. Investigations show that as quickly as a new vulnerability or a new virus is detected or launched, the consequences can be comprehensive. We will not go further into this subject, because there are many investigation reports which confirm these claims. The question is whether organisations are able to handle these challenges. We believe that systematics, maturity and efficiency are some of the key factors for handling these challenges and that BS 7799 (ISO/IEC 17799) is able to contribute regarding the implementation of these important factors.

There is strong reason to believe that interoperability between organisations will become more important in the future. A common regime in how to handle the IS challenge will then be of importance.

Will organisations that are certified according to BS 7799, or using the standard informally, have better capability for preventing, detecting and responding to security breaches in contrast to organisations which have based their ISMS on other kinds of ISMS, or those who do not have an ISMS at all?

1.3 Motivation/significance

Information, supporting processes, systems, networks, employees and management are all important business assets. Confidentiality, integrity and availability of information may be essential in maintaining competitive edge, cash flow, profitability, legal compliance and commercial image. Increasingly, organisations and their information systems and networks are faced with security threats

from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated [4].

A dependence on information systems and services means that organisations are more vulnerable to security threats. The security that can be achieved through technical means is limited, and it should be supported by appropriate management and procedures. Information security within organisations is handled today by many different regimes, management systems and procedures. The exchange of knowledge and experience between organisations regarding the different information security regimes has been done.

In the last years the various security management systems as such;

- "The Forum's Standard of Good Practice" issued by Information Security Forum [28] and
- "COBIT Management Guidelines" issued by COBIT Steering Committee and the IT Governance Institute [9]

have become more easily available.

The Organisation for Economic Co-operation and Development (OECD) has also demonstrated interest in the IS area. The guideline "OECD Guidelines for the Security of Information Systems and Networks Towards a Culture of Security" [24] has been issued.

Interactions and the exchange of information between organisations have increased largely in the last few years and it is likely that a further increase will happen. It is an assumption that the information community will be more open in the future. To manage the IS in a sufficient way, it will be vital to do it according to well-known processes, and approved standards, with well defined principles across organisational boundaries.

These standards and guidelines have many similarities and are partly based on each other. Only one of the standards can be regarded as an international standard, BS 7799 [4, 13]. This is the only standard which offers international certification possibilities. The differences between interacting organisations and business sectors are comprehensive. It is a question whether the security regimes, based on different standards and guidelines, are an obvious weakness for the IS within the specific organisation. The degree of security will depend on the weakest link.

Today, the ownership of companies, and even large companies, changes from one day to another. There may be reasons to believe that in the years to come the status regarding the security management regime, will influence the price of the company and will be an important issue in the due diligence process.

Previous research [16, 20, 23] concludes that it is important to notice that apart from the process for achieving the certificate, it is from then on that it may be possible to achieve real advantages regarding improvements.

1.4 Research questions

The following research questions are defined:

1. What problem shall the BS 7799 standard solve?
2. How many organisations are certified according to BS 7799?
3. What kinds of organisations are certified according to BS 7799?
4. To what extent have organisations using BS 7799 solved the problem?

Each of the research questions are discussed in the chapters 2.1.1 to 2.1.4.

1.5 Searching for literature

Searching after literature in scientific databases has been made possible through the services provided by the library at Gjøvik University College. The services include the possibility of remote access to scientific databases via the OpenSSH facility. The following databases have been used among others, Springer Link, CiteSeer.IST, Science Direct and ISI Web of Science.

2. Background and theory

The first part of this chapter covers related work and the state of art regarding the research questions. The rest of the chapter is about relevant theory.

2.1 Related work and state of the art

In this chapter the research questions defined in chapter 1.4 are discussed.

2.1.1 Information and definition about the problem that the BS 7799 standard shall solve

The BS 7799 standard [4], p.1, itself defines the problem that the standard shall solve.

“This British Standard promotes the adoption of a process approach for establishing, implementing, operating, monitoring, maintaining and improving the effectiveness of an organization’s ISMS.

An organization must identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs, can be considered to be a process. Often the output from one process directly forms the input to the following process.

The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a “process approach”.

A process approach encourages its users to emphasize the importance of:

- a) understanding business information security requirements and the need to establish policy and objectives for information security;*
- b) implementing and operating controls in the context of managing an organization’s overall business risk;*
- c) monitoring and reviewing the performance and effectiveness of the ISMS;*
- d) continual improvement based on objective measurement.”*

A number of other articles emphasise the significance of having certified management systems, regarding quality and information security.

The last edition of the BS 7799 standard has been produced to harmonize it with other management system standards such as ISO 9001:2000 and ISO 14001:1996 in order to provide consistent and integrated implementation and operation of management systems. It also introduces a Plan-Do-Check-Act (PDCA) model as part of a management system approach to developing, implementing, and improving the effectiveness of an organisation’s ISMS. The implementation of the PDCA model will also reflect the principles as set out in the OECD guidance (2002) governing the security of information systems and networks. In particular, this edition gives a robust model for implementing the principles in those guidelines which govern risk assessment, security design and implementation, security management and reassessment.

The BS 7799 standard has been prepared for business managers and their staff in order to provide a model for setting up and managing an effective ISMS. The adoption of an ISMS should be a strategic decision for an organisation. The design and implementation of an organisation’s ISMS is influenced by business needs and objectives, resulting security requirements, the processes employed and the size and structure of the organisation. These and their supporting systems are expected to change over time. It is expected that simple situations require simple ISMS solutions. The standard [4] can be used

by internal and external parties, including certification bodies, to assess an organisation's ability to meet its own requirements, as well as any customer or regulatory demands.

The paper "A study on the certification of the information security management system" [1] mentions the main goal of international standardisation. The goal is to create a trade environment providing each of the following 6 functions for promoting the exchange of products:

1. Product quality and reliability and price concordance.
2. Guaranteeing the user's security and promoting the recycling of resources.
3. Goods, technology and service interoperability and mutual sequential continuity.
4. Simplification in order to reduce moulding for a greater production capacity and thereby to reduce costs.
5. Simplification in order to diminish the frequency of modelling in the hope of expanding production scope and lower costs.
6. Improving the convenience of repair and maintenance and distribution efficiency.

Conclusion: The problem which the standard shall solve **is defined by the standard itself** and in relevant papers. The BS 7799 standard shall also provide a model for setting up and managing an effective ISMS.

2.1.2 How many organisations are certified according to BS 7799-2?

The ISMS International User Group [14] maintains an international register directory. So far, i.e. June 2004, nearly 800 organisations worldwide have been certified according to BS 7799-2. The register gives an overview of certified organisations and certification bodies. Nine organisations are certified according to BS 7799-2 in Norway.

The KvaLex database [3] contains information about Norwegian organisations which are certified according to BS-7799-2.

Conclusion: The ISMS international User Group [14] and the KvaLex database [3] both confirm that **9 Norwegian organisations are certified** according to BS 7799-2. One of the certified organisations is the author's employer, VincIT. VincIT is therefore legal disqualified and will be leaved out from the planned survey.

2.1.3 What kinds of organisations are certified according to BS 7799?

As mention in 2.1.2, the ISMS International User Group [14] maintains an international register directory. The register gives an overview of certified organisations. Information about these organisations can be found on the World Wide Web and is sorted into defined categories.

The main category of the certified organisations in Norway is presented in chapter 4.1.1. Organisations within the category "Telecommunication and IT" constitute six out of nine organisations.

Conclusion: Organisations within **Telecommunication and IT** constitute six out of nine organisations in Norway.

2.1.4 To what extent have organisations using BS 7799 solved the problem?

This question is the most challenging, of the four research questions, and we have not found any empirical data which answer this question.

IS and quality are two important aspects of the same matter. This statement is also a part of the book, “Handbook in data security “ (Norwegian: *Håndbok i datasikkerhet*) [27]. Annex C in the BS 7799-2 [4] standard has made an informative correspondence between the three standards

- BS EN ISO 9001:2000,
- BS EN ISO 14001:1996 and
- BS 7799-2:2002.

From the table we see that the correspondence between ISO 9001 and BS 7799-2 are very obvious. A lot of other papers point out the relation between quality and information security. Quality- and security management systems may be managed and maintained in the same management regime.

We have found many papers regarding the problem that the certification of organisation’s quality systems shall solve and the effect of introducing quality systems into organisations. ISO 9000 is the most conspicuous quality system that is treated in addition to Total Quality Management (TQM). We have also found papers about combine process certification and product evaluation. The papers about quality systems point out “maturity” as an important factor for the organisation in order to utilize the goals of the standards.

In paper [23] the topic was “The longitudinal effects of the ISO 9000 certification process on business performance”. The conclusions in the paper were based on information collected in a cross-sectional study undertaken in Australia regarding ISO 9000 quality certification processes. The findings show that the motive for adopting ISO 9000 certification and the **maturity** of the quality culture are significant predictors of the benefits derived from ISO 9000 certification. Another conclusion in the paper was that organizations that have been audited to the ISO 9000 standards believe that the quality audit process contributes to business performance when the quality culture in the organization is well developed and when the manager’s motivation to gain certification has been to improve business performance and not to conform to an international standard. The individual element which was found to contribute most to business performance was customer focus.

The article “An approach to combine process certification and product evaluation” [21], addresses the question whether it would be possible to ‘marry’ concepts such as product and/or systems evaluation and process certification and, if so, how this would impact on the IS status of an organisation. This question will not be addressed in this thesis, but it is an interesting question which may have influence on the success of BS 7799 certification. Process certification and product evaluation may be a holistic approach towards adequate IS.

“Working conditions and effect of ISO 9000 in six furniture-making companies: implementation and processes” [16] deals with many aspects in connection with ISO 9000 certification. The most interesting findings were that ISO 9000 implementation must be considered as a change process where not only the technical but also the political and cultural sides need to be dealt with. The value of implementing ISO 9000 can be increased by identifying and introducing additional goals besides certification and enhancing the change process, sometimes by adding minor extra resources.

The article “Trust through evaluation and certification?” [10], explores three main theories in connection with information and IT security. Do evaluation, certification, and standardization serve in creating trust by reducing complexity in such a way that they can be understood and verified by the user? This article discusses “trust” over several pages and in the end some statements are made about the meaning of it. To what extent it is correct to assume that trust is automatically achieved if a certain level is attained is also discussed.

The article “A critical look at ISO 9000 software quality management” [11] explains the contents in the ISO 9000 family and which standard should be used to specific needs. Empirical surveys have been performed in software suppliers that have gathered experience with the implementation of ISO 9000 based quality systems. The findings of the surveys are described in detail in other papers, but the findings in these surveys are summarized in this paper. The most interesting recommendation is the

following [11], p.78: *"The lack of empirical evidence justifying key assumptions and suggestions of ISO 9000 for software development is probably one of the most important weaknesses of the standards. Software quality management concepts should be based on empirical evidence, whenever possible. Standardization bodies would probably be the most appropriate institutions to initiate, to support, and to co-ordinate empirical research work"*.

M. C. Paulk has written an article [20] based on participation at several workshops and site visits in software organisations at maturity level 4 and 5. The maturity level of organisations are explained in chapter 2.3 The maturity model.

A survey was distributed in order to informally test the anecdotal observations about high maturity practices, [20] p.4. *"Eleven out of thirteen of the organisations surveyed had ISO 9001 certification. High maturity organisations generally emphasize openness, communication, and a commitment to quality and the customer at all levels. They encourage a process orientation in their staff. Worker empowerment and participation in process definition and improvement activities are real; process improvement is part of everyone's job. There is a "quality culture" in high maturity organizations. Rewards and incentives are established for process improvement efforts, and worker empowerment and participation are more than just slogans. High maturity organizations recognize the importance of good staff."*

M. C. Paulk claims also that, [20] p.5: *"It is very difficult to be a high maturity supplier if you have a low maturity customer (or low maturity suppliers or partners, in the case of strategic alliances, joint ventures, and virtual organizations)."*

Conclusion: We have not found any articles which discuss or answer our research question directly. There are many research articles regarding ISO 9000 and also about security evaluation according to TCSEC, ITSEC, CC and other similar evaluation and certification schemes. Some of the articles are based on empirical surveys of the ISO 9000 family of standards. Despite of that, the authors of these articles specify that more empirical surveys are needed. A lot of interesting questions and effects after performing a quality certification scheme were noticed.

The research question is not sufficiently identified in the available literature and we decide to carry out a survey to collect data about the effects of implementing BS 7799 and an ISMS.

2.2 BS 7799 and Information Security Management System (ISMS)

The work to establish ISMS can be traced back to November 1987 and is to be found at the Gamma Secure Systems Limited websites [12]:

"The origin of ISO/IEC 17799 goes back to the days of the UK Department of Trade and Industry's (DTI) Commercial Computer Security Centre (CCSC). Founded in May 1987, the CCSC had two major tasks. The first was to help vendors of IT security products by establishing a set of internationally recognised security evaluation criteria and an associated evaluation and certification scheme. This ultimately gave rise to the ITSEC and the establishment of the UK ITSEC Scheme. The second task was to help users by producing a code of good security practice and resulted in a "Users Code of Practice" that was published in 1989. This was further developed by the National Computing Centre (NCC), and later a consortium of users, primarily drawn from British Industry, to ensure that the Code was both meaningful and practical from a users point of view. The final result was first published as a British Standard's guidance document PD 0003, A code of practice for information security management, and following a period of further public consultation recast as British Standard BS7799:1995. A second part BS7799-2:1998 was added in February 1998. Following an extensive revision and public consultation period, that began in November 1997, the first revision of the standard, BS7799:1999 was published in April 1999. Part 1 of the standard was proposed as an ISO standard via the "Fast Track" mechanism in October 1999, and published with minor amendments as

ISO/IEC 17799:2000 on 1st December 2000. BS 7799-2:2002 was officially launched on 5th September 2002.”

The article “A study on the certification of the information security management system” [1] , p. 450, describes the history of ISMS in a section intended as a brief introduction to related information security management specifications.

“How should the Common Body of Knowledge (CBK) of the specialized personnel working with information security be accredited? An organisation specialized in the accreditation of information security personnel, the International Information System Security Certification Consortium (ISC)² was established in Salisbury, England. To be approved by the (ISC)², one requires tests of 10 major CBK categories (taking normally 6 h to answer 250 multiple-choice questions). Correct answers to 70% of the questions in combination with a minimum of 3 years working experience with information security related matters are needed to qualify as a Certified Information Systems Security Professional (CISSP). CISSP certification is not issued on a permanent basis, but the test must be taken once every 3 years, and only after passing the test will the person get a renewed certificate. The Canadian Information Processing Society (CIPS), the Computer Security Institute (CSI), and the Information Systems Security Association (ISSA) all recognize CISSP certification. Apart from (ISC)², SANS and other organisations also have their series of accreditation tests for specialized information security techniques (e.g., UNIX Security, Intrusion Detection Systems). Apart from the certification of specialized information security personnel, the work to set the international standards for the specifications for the management of information systems security is in progress.

The ideas behind and the structure of the specifications for information security management certification are the same as for ISO 1400, as shown in Figure 1: Systematized security concepts [1]. Systematized security concepts such as main requirements, goal management, risk prevention, law obedience, and continuous improvement are implemented according to a Plan–Do–Check–Action (P–D–C–A) cycle as shown in Figure 2: The risk management model.”

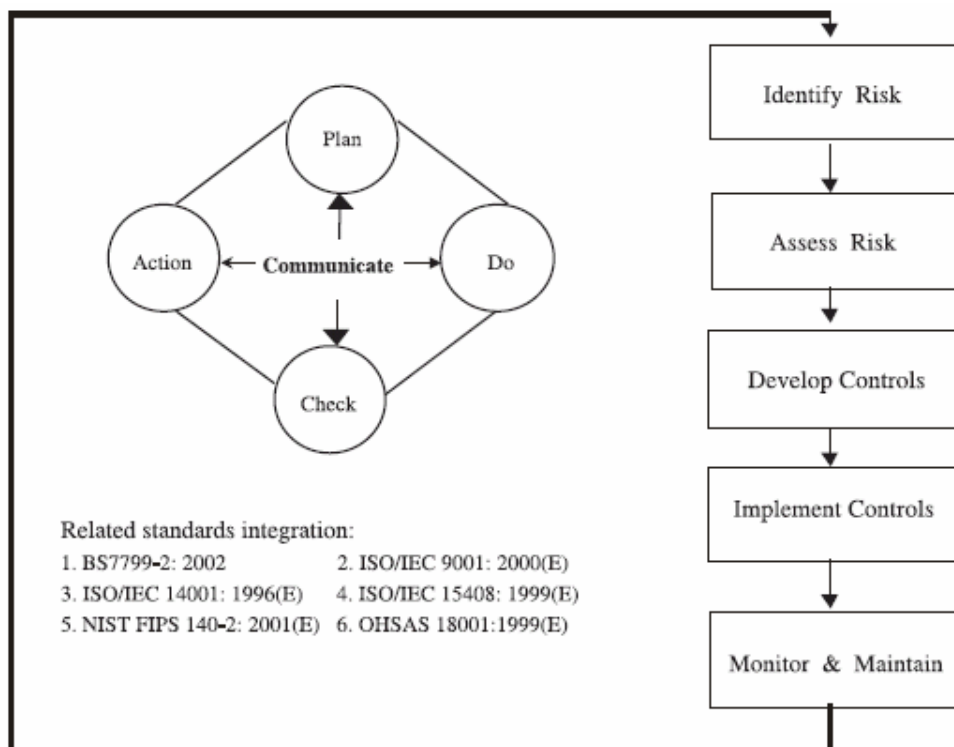


Figure 1: Systematized security concepts [1]

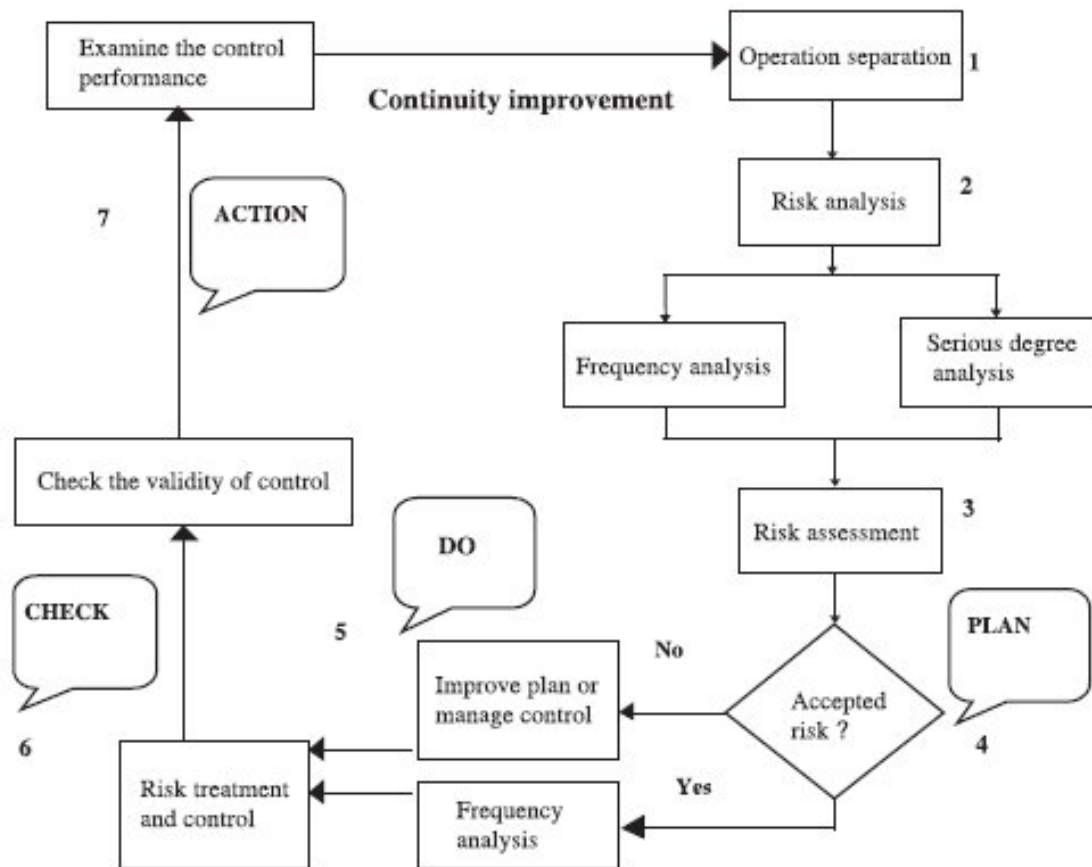


Figure 2: The risk management model [1]

“Since risk appraisal includes all organisations and all departments, areas, staff and activities, the rationality and conformity of the appraisal is still a topic for research. Compared to ISO 14001, it is more difficult.” [1] p.450.

BS 7799-2:2002 [4] has perhaps a more well-arranged diagram to explain the Plan-Do-Check-Act model. As stated in [4] p.1:

“The application of a system of processes within an organisation, together with the identification and interactions of these processes, and their management, can be referred to as a “process approach”.

A process approach encourages its users to emphasize the importance of:

- a) understanding business information security requirements and the need to establish policy and objectives for information security;
- b) implementing and operating controls in the context of managing an organisation’s overall business risk;
- c) monitoring and reviewing the performance and effectiveness of the ISMS;
- d) continual improvement based on objective measurement.”

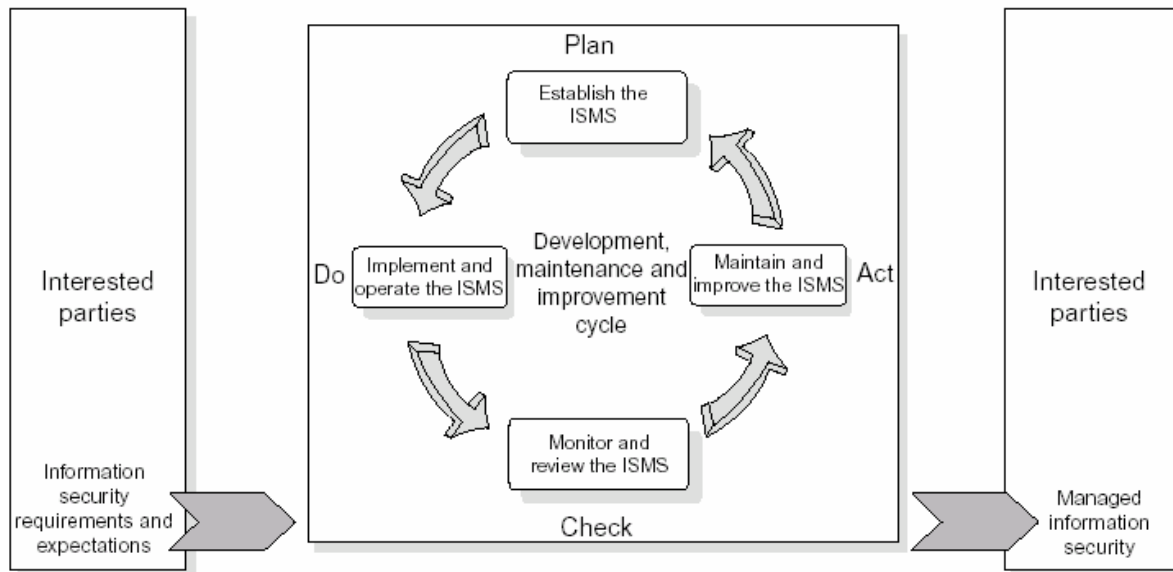


Figure 3: PDCA model applied to ISMS processes [4]

BS 7799-2:2002 [4] p.2:

“Plan (establish the ISMS)”

Establish security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organisation’s overall policies and objectives.

Do (implement and operate the ISMS)

Implement and operate the security policy, controls, processes and procedures.

Check (monitor and review the ISMS)

Assess and, where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review.

Act (maintain and improve the ISMS)

Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the ISMS.”

The standard [4] is aligned with BS EN ISO 9001:2000 and BS EN ISO 14001:1996 in order to support consistent and integrated implementation and operation with related management standards.

2.3 The maturity model

The Capability Maturity Model for Software was developed at Carnegie Mellon Software Engineering Institute. The Capability Maturity Model for Software (also known as the CMM and SW-CMM) has been a model for judging the maturity of the software processes, regarding development and maintenance, of an organisation for many years. The model helped organisations to identify the key practices required to help them increase the maturity of these processes.

The model may be illustrated as a staircase with five steps.

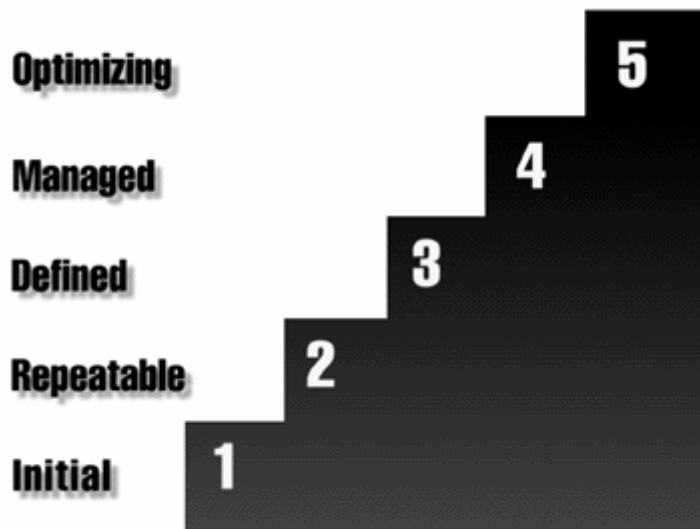


Figure 4: The Capability Maturity Model for Software [6]

A brief summary of the Capability Maturity Model for Software (SW-CMM) is described at the website of the Carnegie Mellon Software Engineering Institute [7]:

“The Capability Maturity Model for Software describes the principles and practices underlying software process maturity and is intended to help software organisations improve the maturity of their software processes in terms of an evolutionary path from ad hoc, chaotic processes to mature, disciplined software processes. The CMM is organized into five maturity levels:

- 1) Initial.** *The software process is characterized as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort and heroics.*
- 2) Repeatable.** *Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.*
- 3) Defined.** *The software process for both management and engineering activities is documented, standardized, and integrated into a standard software process for the organisation. All projects use an approved, tailored version of the organisation's standard software process for developing and maintaining software.*
- 4) Managed.** *Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.*
- 5) Optimizing.** *Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.*

Predictability, effectiveness, and control of an organisation's software processes are believed to improve as the organisation moves up these five levels. While not rigorous, the empirical evidence to date supports this belief.

Except for Level 1, each maturity level is decomposed into several key process areas that indicate the areas an organisation should focus on to improve its software process.

The key process areas at Level 2 focus on the software project's concerns related to establishing basic project management controls. They are Requirements Management, Software Project Planning, Software Project Tracking and Oversight, Software Subcontract Management, Software Quality Assurance, and Software Configuration Management.

The key process areas at Level 3 address both project and organisational issues, as the organisation establishes an infrastructure that institutionalizes effective software engineering and management processes across all projects. They are Organisation Process Focus, Organisation Process Definition, Training Program, Integrated Software Management, Software Product Engineering, Intergroup Coordination, and Peer Reviews.

The key process areas at Level 4 focus on establishing a quantitative understanding of both the software process and the software work products being built. They are Quantitative Process Management and Software Quality Management.

The key process areas at Level 5 cover the issues that both the organisation and the projects must address to implement continual, measurable software process improvement. They are Defect Prevention, Technology Change Management, and Process Change Management.

Each key process area is described in terms of the key practices that contribute to satisfying its goals. The key practices describe the infrastructure and activities that contribute most to the effective implementation and institutionalization of the key process area.”

The technical report, from the Software Engineering Institute at Carnegie Mellon University, Capability Maturity Model for Software [18] provides an overview of the latest version of the Capability Maturity Model for Software, CMM v1.1. Through more than six years of experience with software process improvement and contributions from hundreds of reviewers, CMM v1.1 describes the software engineering and management practices that characterise organisations as they mature their processes for developing and maintaining software. The need for a process maturity framework to prioritise improvement actions is stressed in the paper [18]. The process maturity framework of five maturity levels and the associated structural components are described and future directions for the CMM are discussed.

The technical report “Key practices of the Capability Maturity Model” [19] provides a technical overview of the Capability Maturity Model for Software and reflects Version 1.1. The process maturity framework of five maturity levels, the structural components that comprise the CMM, how the CMM is used in practice, and future directions of the CMM are described.

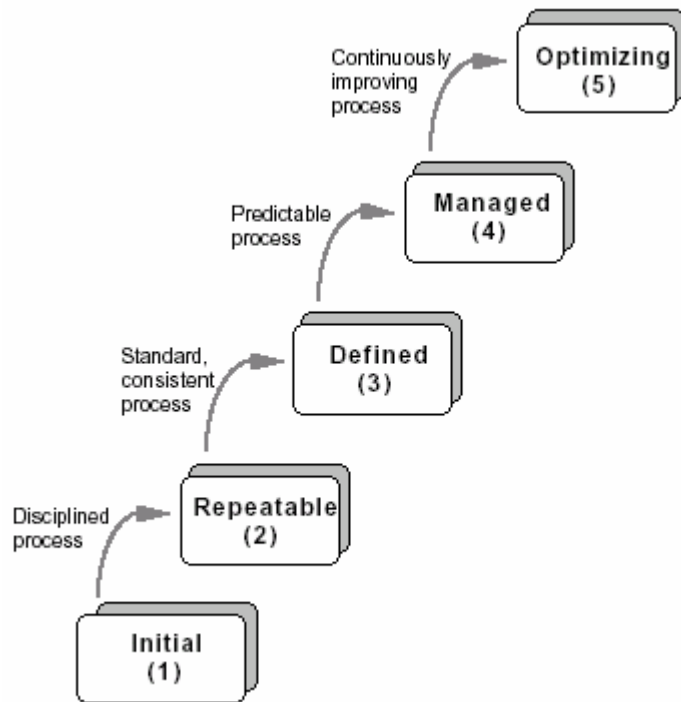


Figure 5: The five levels of software process maturity [18]

2.3.1 More about the five levels of software process maturity

Visibility into the project status and performance afforded to management at each level of the process maturity may be illustrated in Figure 6. Each succeeding maturity level incrementally provides better visibility into the software process. Usually software engineers have detailed insight into the state of a project because they have first-hand information on project status and performance. When it comes to large projects, of software engineers, the detailed insight will usually be reduced to only cover their own area of responsibility. Those outside the project without first-hand exposure, such as senior managers, lack visibility into the project's processes and rely on periodic reviews for the information they require in order to monitor progress.

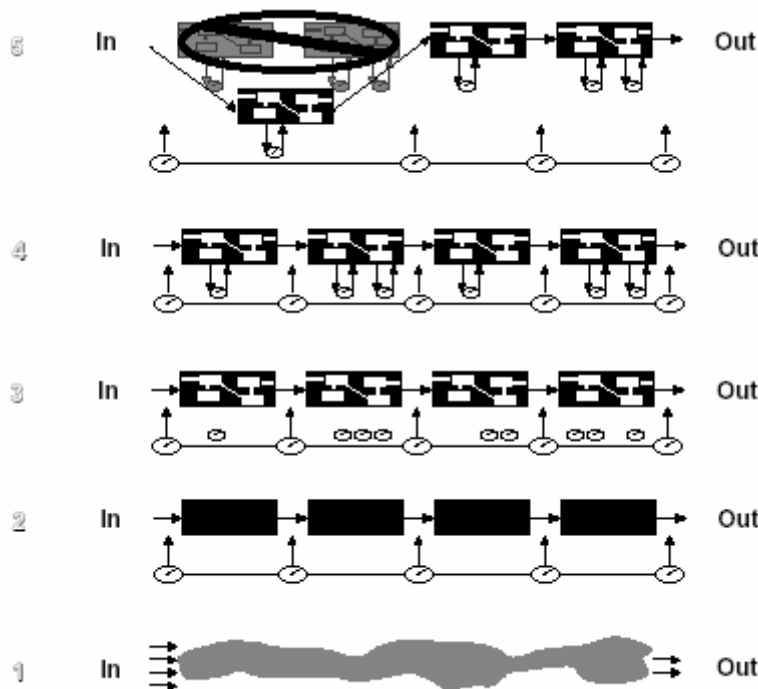


Figure 6: A management view of visibility into the software process at each maturity level [18]

The levels are explained in the paper [18] p.20:

“At Level 1, the software process is an amorphous entity – a black box – and visibility into the project's processes is limited. Since the staging of activities is poorly defined, managers have an extremely difficult time establishing the status of the project's progress and activities¹. Requirements flow into the software process in an uncontrolled manner, and a product results. Software development is frequently viewed as black magic, especially by managers who are unfamiliar with software.

At Level 2, the customer requirements and work products are controlled, and basic project management practices have been established. These management controls allow visibility into the project on defined occasions. The process of building the software can be viewed as a succession of black boxes that allows management visibility at transition points as activity flows between boxes (project milestones). Even though management may not know the details of what is happening in the box, the products of the process and checkpoints for confirming that the process is working are identified and known. Management reacts to problems as they occur.

At Level 3, the internal structure of the boxes, i.e., the tasks in the project's defined software process, is visible. The internal structure represents the way the organisation's standard software process has been applied to specific projects. Both managers and engineers understand their roles and responsibilities within the process and how their activities interact at the appropriate level of detail. Management proactively prepares for risks that may arise. Individuals external to the project can obtain accurate and rapid status updates because defined processes afford great visibility into project activities.

At Level 4, the defined software processes are instrumented and controlled quantitatively. Managers are able to measure progress and problems. They have an objective, quantitative basis for making

¹ This leads to the Ninety-Ninety Rule: 90% of the project is complete 90% of the time.

decisions. Their ability to predict outcomes grows steadily more precise as the variability in the process grows smaller.

At Level 5, new and improved ways of building the software are continually tried, in a controlled manner, to improve productivity and quality. Disciplined change is a way of life as inefficient or defect-prone activities are identified and replaced or revised. Insight extends beyond existing processes and into the effects of potential changes to processes. Managers are able to estimate and then track quantitatively the impact and effectiveness of change."

2.3.2 COBIT and Management Guidelines

The Information Systems Audit and Control Foundation, IT Governance Institute and the sponsors of COBIT: Control Objectives for Information and related Technology have designed and created the publication Management Guidelines [9]. The guideline is a part of a framework which also includes the Executive Summary, Framework, Control Objectives and Implementation Tool Set.

The Management Guidelines [9] p.5:

"COBIT stands for Control Objectives for Information and related Technology and is an open standard for control over information technology, developed and promoted by the IT Governance Institute. This framework identifies 34 information technology (IT) processes, a high-level approach to control over these processes, as well as 318 detailed control objectives and audit guidelines to assess the 34 IT processes. It provides a generally applicable and accepted standard for good IT security and control practices to support management's needs in determining and monitoring the appropriate level of IT security and control for their organisations. The IT Governance Institute has further built on this with leading-edge research, in cooperation with world-wide industry experts, analysts and academics. This has resulted in the definition of Management Guidelines for COBIT, which consist of Maturity Models, Critical Success Factors (CSFs), Key Goal Indicators (KGIs) and Key Performance Indicators (KPIs)."

The maturity model used in COBIT for control over IT processes consists of developing a method of scoring so that an organisation can grade itself from non-existent to optimised (from 0 to 5). The approach has been derived from the Maturity Model for software development capability, defined by Software Engineering Institute

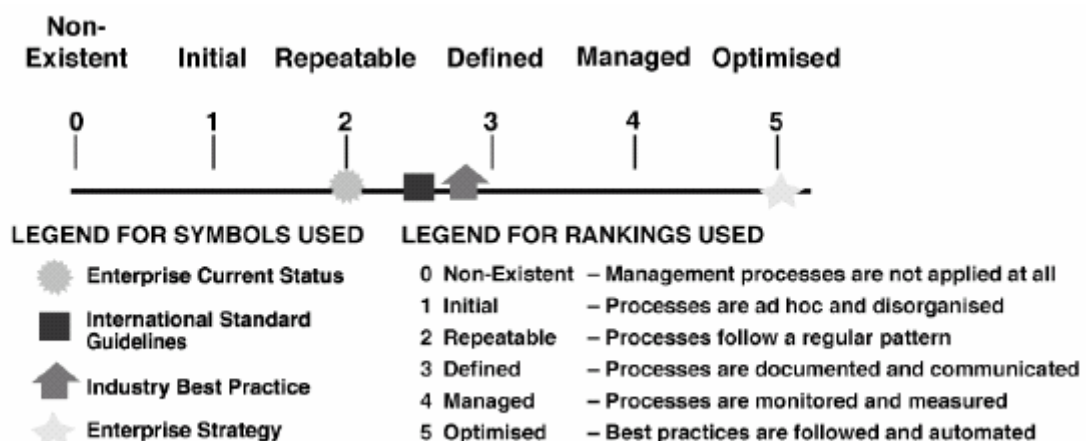


Figure 7: Process Maturity Model scoring from 0 to 5 [9]

2.3.3 Maturity of information risk management

The papers, "Information Security Governance" [26] and "A study on the certification of the information security management systems" [1], are both based on the method and theory presented in the maturity models developed at Software Engineering Institute Carnegie Mellon University, COBIT Steering Committee and the IT Governance Institute.

Both papers contain a layout of a table where the conditions for the maturity levels are defined. The following table is fetched from the two papers:

Table 1: Maturity of information risk management [1, 26]

Maturity level	Description
0	Non-existent: management processes are not applied at all
	(a) No risk assessment of processes or business decisions. The organisation does not consider the business impact associated with security vulnerabilities. Risk management has not been identified as relevant to IT solutions and services;
	(b) The organisation does not recognize the need for IT security. Responsibilities and accountabilities for security are not assigned. Measures supporting the management of IT security are not implemented. There is no IT security reporting or response process for IT security breaches. No recognizable security administration processes exist;
	(c) No understanding of the risks, vulnerabilities and threats to IT operations or service continuity by management. 1 Initial/Ad-Hoc: processes are ad-hoc and disorganized
1	Initial/Ad-Hoc: processes are ad-hoc and disorganized
	(a) The organisation consider IT risks in an ad hoc manner, without following defined processes or policies. Informal project based risk assessment is used;
	(b) The organisation recognizes the need for IT security, but security awareness depends on the individual. IT security is reactive and not measured. IT security breaches invoke 'finger pointing' responses if detected, because responsibilities are unclear. Responses to IT security breaches are unpredictable;
	(c) Responsibilities for continuous service are informal, with limited authority. Management is becoming aware of the risks related to and the need for continuous service.
2	Repeatable but intuitive: processes follow a regular pattern
	(a) There is an emerging understanding that IT risks are important and need to be considered. Some approach to risk assessment exists, but the process is still immature and developing;
	(b) Responsibilities and accountabilities for IT security are assigned to an IT security coordinator with no management authority. Security awareness is fragmented and limited. Security information is generated, but is not analyzed. Security tends to respond reactively to incidents and by adopting third-party offerings, without addressing the specific needs of the organisation. Security policies are being developed, but inadequate skills and tools are still being used. IT security reporting is incomplete or misleading;
	(c) Responsibility for continuous service is assigned. Fragmented approach to continuous service. Reporting on system availability is incomplete and does not take business impact into account.
3	Defined process: processes are documented and communicated
	(a) An organisation-wide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff;
	(b) Security awareness exists and is promoted by management through formalized briefings. IT security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for IT security are assigned, but not consistently enforced. An IT security plan exists, driving risk analysis and security solutions. IT security reporting is IT focused, rather than business focused. Ad hoc intrusion testing is performed;
	(c) Management communicates consistently the need for continuous service. High-availability components and system redundancy are being applied piecemeal. An inventory of critical systems and components is rigorously maintained.

Maturity level	Description
4	Managed and measurable: processes are monitored and measured
	(a) The assessment of risk is a standard procedure and exceptions would be noticed by IT management. It is likely that IT risk management is a defined management function with senior level responsibility. Senior management and IT management have determined the levels of risk that the organisation will tolerate and have standard measures for risk/return ratios;
	(b) Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and practices are completed with specific security baselines. Security awareness briefings, user identification, authentication and authorization have become mandatory and standardized. Intrusion testing is standardized and leads to improvements. Cost/benefit analysis, is increasingly used. Security processes are coordinated with the overall organisation security function and reporting is linked to business objectives;
	(c) Responsibilities and standards for continuous service are enforced. System redundancy practices, including use of high-availability components, are being consistently deployed.
5	Optimized-best practices are followed and automated
	(a) Risk assessment has developed to the stage where a structured, organisation-wide process is enforced, followed regularly and well managed;
	(b) IT security is a joint responsibility of business and IT management and integrated with corporate business objectives. Security requirements are clearly defined, optimized and included in a verified security plan. Functions are integrated with applications at the design stage and end users are increasingly accountable for managing security. IT security reporting provides early warning of changing and emerging risk, using automated active monitoring approaches for critical systems. Incidents are promptly addressed with formalized incident response procedures supported by automated tools. Periodic security assessments evaluate the effectiveness of implementation of the security plan. Information on new threats and vulnerabilities is systematically collected and analyzed, and adequate mitigating controls are promptly communicated and implemented. Intrusion testing, root cause analysis of security incidents and proactive identification of risk is the basis for continuous improvements. Security processes and technologies integrated organisation wide;
	(c) Continuous service plans and business continuity plans are integrated, aligned and routinely maintained. Buy-in for continuous service needs is secured from vendors and major suppliers.

In the article [1] the ISMS certification is divided into five categories, as shown in Table 2. This is based on the management concept shown in Table 1 “Maturity of information risk management”, ISO regulations [15] which have been adopted in many countries and the article “Incremental information security certification” [5].

Category 3 and above connects to the certification of the international BS7799-2. Category 4 is designed to take differing industry demands into consideration. Category 5, apart from the requirements in BS7799-2, also has to consider the integrity of information security management systems and quality and environmental management systems.

Table 2: The classification of certification in the ISMS [1]

Categories	Requirements for certification
1	(a) Compliance with legal requirements (BS 7799-2: 1999, 4.10.1). (b) Security policy (BS 7799-2: 1999, 4.1). (c) Asset classification and control (BS 7799-2: 1999, 4.3). (d) Protection against malicious software (BS 7799-2: 1999, 4.6.3). (e) Security in development and support processes (BS 7799-2: 1999, 4.8.5).
2	(a) Requirements for Categories 1. (b) Compliance (BS 7799-2: 1999, 4.10). (c) Organisational security (BS 7799-2: 1999, 4.2). (d) User training (BS 7799-2: 1999, 4.4.2). (e) Responding to security incidents and malfunctions (BS 7799-2: 1999, 4.4.3). (f) Business continuity management (BS 7799-2: 1999, 4.9).
3	Requirements for BS 7799-2:2002 Annex A.
4	Requirements for BS 7799-2:2002 Annex A as well as requirements for different industries as shown in Fig. 8 (Article [1].)
5	Requirements for TQM (Total quality management, included BS 7799-2).

The PDCA-cycle is mentioned in chapter 2.2 BS 7799 and Information Security Management System (ISMS). Article [1], at p.460, contains a table where the PDCA-cycle, the maturity categories and requirements for risk level are summarized, see Table 3.

Table 3: The international ISMS standards in risk management cycle [1]

Risk management level		Requirements for risk level
Cycle	Categories	
Plan		ISO/IEC TR 13335
Do	1	ISO/IEC 17799
	2	ISO/IEC 17799
	3	ISO/IEC 17799
	4	ISO/IEC 17799 plus industry-related standards (e.g., Health informatics - Public Key Infrastructure (PKI) must comply with ISO/TS 17090, too)
	5	The integration of ISO/IEC 17799, industry-related standards, ISO 9000, and ISO 14000 into ISMS
Check		BS 7799-2:2002
Action		The standards listed in Fig. 5, in article [1]

The article [1] has a reference to a "Fig. 5". The standard mention is: ISO/IEC 15408:1999, ISO/IEC 15026:1998, ISO/IEC 17799:2000, ISO/IEC TR 15504:1998, ISO/IEC 21287:2002, the computer process personal data protection act.

2.4 Security Metrics Guide for Information Technology Systems

Maturity is also a subject in the "Security metrics guide for information technology system, NIST 800-55 [22]" published as a special publication in 2003 [22].

The guide states that the maturity of an organization's IT security program determines the type of metrics that can be gathered successfully.

Section 3.3 in the paper [22] p.11 explains the relation between an organisation's maturity and how the security metrics are developed and improved when the maturity increases.

“A program’s maturity is defined by the existence and institutionalization of processes and procedures. As a security program matures, its policies become more detailed and better documented, the processes that it uses become more standardized and institutionalized, and it produces data that can be used for performance measurement in greater quantity. According to NIST SP 800-26, the security program progresses from having policies (Level 1) to having detailed procedures (Level 2), implementing these procedures (Level 3), testing compliance with and effectiveness of the procedures (Level 4), and finally fully integrating policies and procedures into daily operations (Level 5). A mature program normally deploys multiple tracking mechanisms to document and quantify various aspects of its performance. As more data becomes available, the difficulty of measurement decreases, and the ability to automate data collection increases. Data collection automation depends on the availability of data from automated sources versus the availability of data from people. Manual data collection involves developing questionnaires and conducting interviews and surveys with the organization’s staff.

More useful data becomes available from semi automated and automated data sources, such as self-assessment tools, certification and accreditation (C&A) databases, incident reporting and response databases, and other data sources as a security program matures. Metrics data collection is fully automated when all data is gathered by using automated data sources without human involvement or intervention.

The types of metrics (implementation, efficiency and effectiveness, and impact) that can realistically be obtained and that can also be useful for performance improvement depend on the maturity of the security control implementation. Although different types of metrics can be used simultaneously, the primary focus of IT security metrics shifts as the implementation of security controls matures. When security controls have been defined in procedures and are in the process of being implemented, the primary focus of metrics will be on the level of implementation of security controls. Examples of implementation metrics that are applied at this level of maturity are the percentage of systems with approved security plans and the percentage of systems with password policies configured as required. When a system progresses through Level 1 and Level 2, the results of these metrics will be less than 100 percent, indicating that the system has not yet reached Level 3. When the metrics implementation results reach and remain at 100 percent, it can be concluded that the system has fully implemented security controls and has reached Level 3.

As security controls are documented and implemented, the ability to reliably collect the outcome of their implementation improves. As an organization’s IT security program evolves and performance data becomes more readily available, metrics will focus on program efficiency - timeliness of security service delivery and effectiveness - operational results of security control implementation. Once security is integrated into an organization’s processes, the processes become self-regenerating, measurement data collection becomes fully automated, and the mission or business impact of security-related actions and events can be determined by data correlation analysis.

The metrics at Level 4 and Level 5 concentrate on measuring effectiveness and efficiency of implemented security controls and the impact of these controls on the organization’s mission. These metrics concentrate on the evidence and results of testing and integration. Instead of measuring the percentage of approved security plans, these metrics concentrate on validating whether security controls, described in the security plans, are effective in protecting the organization’s assets. For example, computing the percentage of crackable passwords within a predefined time threshold will validate the effectiveness of an organization’s password policy by measuring the length of time required to break policy-compliant passwords. The impact metrics would quantify incidents by type (e.g., root compromise, password compromise, malicious code, denial of service) and correlate the incident data to the percentage of trained users and system administrators to measure the impact of training on security.”

3. Survey

The purpose of the survey is to measure any correlations between occurred consequences, information security breaches and the maturity level of the ISMS within the organisation.

3.1 Choice of method

One of the goals in this thesis is to find out what kind of data are available regarding the measurement of the effects of implementing BS 7799. By implementing BS 7799 we mean either informal use of the standard or a formal certification according to the requirements in the standard.

The books "Craft of Research" [30] and "Research Design, Qualitative, Quantitative and Mixed Methods Approaches" [17] are used as guidance regarding the choice of method and design of this thesis report.

Relative early in the thesis it became clear to us that data and especially empirical data about the effects of BS 7799 implementation were very limited. We have found data and empirical studies from a few ISO 9001 certification schemes. A general conclusion in these findings was the lack of empirical data. Most of these papers point out the need for more empirical data regarding the effects of an ISO 9001 certification.

What kind of statistical data, regarding computer crime, attacks or consequences versus the kind of ISMS in the organisations is available? We have been in contact with the following organisations in Norway, searching for statistical data regarding the issue mention above:

- The Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM)
- Centre for Information Security (Senter for informasjonssikring)
- DNV (Det Norske Veritas)
- The National Institute of Technology, Norway - Certification (Teknologisk institutt Sertifisering as)

None of the organisations could help us with data that were helpful or applicable in solving our main research question.

Then we concluded that we have to try to obtain more data about the effects of using BS 7799 in the organisations. We have to include organisations which have implemented various types of ISMS and organisations which have not implemented any ISMS. We want to compare the "security level" in organisations which have implemented ISMS against organisations which have not implemented any ISMS.

We realised that there were some positions between organisations which are certified and organisations which do not use any ISMS. The organisations may then be categorised as below:

- certified according to BS 7799
- informal use BS 7799
- other ISMS
- own developed ISMS
- do not use any ISMS.

One or a combination of the following processes may be executed to collect the data:

- Technical inspection regarding IS in the organisations
- Interview of personnel regarding IS in the organisations
- Remote testing of the IS in the organisations according to the Open-Source Security Testing Methodology Manual (OSSTMM) [25]

- Internal testing of the IS in the organisations according to OSSTMM [25]
- Distribution of a questionnaire regarding the IS in the organisations.

Remote testing according to OSSTMM [25] may be reduced to testing network surveying, port scanning and denial of service.

An interview of appropriate personnel in a number of organisations, technical inspections and internal testing, would according our consideration, occupy too much time and resources. Remote testing, without inspection or interviewing, would only give us a snapshot regarding the IS status in the organisations. We would not be able to assess e.g. the internal practice. It would probably also have been a challenge to get necessary authorizations to carry out the remote testing.

With the time and resources available in mind, we had to turn down all the alternatives apart from the questionnaire.

When we had decided to carry out a questionnaire we considered doing it by means of a web-application. We were in contact with the ISMS International User Group [14] and Gamma Secure Systems Limited [12] and asked for assistance and help in executing the questionnaire. An automated web application with sufficient security would be of great help in collecting data from organisations worldwide. But, in view of the time and resources available we had to reject the use of the web application.

We decided to carry out a paper based questionnaire because we had to offer anonymity. It was not enough time to implement a web based questionnaire offering sufficient anonymity and security.

3.1.1 Mix method approach

The approach selected in this thesis is a mix of quantitative- and qualitative methods. The approach as “*Mixed methods procedures*” is described in chapter 11 in the book “*Research Design, Qualitative, Quantitative and Mixed Methods Approaches*” [17].

We had decided to carry out a survey in the form of a questionnaire. The target for the questionnaire was Norwegian organisations. The previous chapter lists the alternatives regarding organisations, ISMS and categorising.

After studying the ISMS described in the BS-7799-2 [4] we want the questionnaire to include the following IS aspects.

- the consequences of security breaches which have hit the organisations from 1999 to 2004, estimated as financial loss
- how security breaches are handled in the organisation and the possibilities for us to get access to statistical data regarding security breaches
- which parts of the ISMS are implemented and how they are implemented

The first two aspects, consequences and statistical data regarding security breaches, are considered as quantitative. Handling of security breaches is considered to be a qualitative survey. The last aspect regarding ISMS implementation, and how the ISMS is implemented, is a mix of both qualitative and quantitative survey. Implemented or not is considered to be a qualitative survey and how the ISMS is implemented as a qualitative survey.

The superior method in this survey is considered to be a **mixed method**. All questions will be placed in the same questionnaire and qualitative and quantitative parts of the questionnaire will be implemented concurrently. The priority of the qualitative and quantitative methods is equal and the findings will be integrated at data collection stage. Seen from the respondents the data will be mixed in the answering stage.

The following steps are identified in the mailed questionnaire:

Step 1: Telephone call to check the mood for participating in the survey.

Step 2: First mail-out is the questionnaire, the accompanying letter, the letter of recommendation from the Norwegian Ministry of Trade and Industry and a preaddressed envelope with postage.

Step 3: Telephone call as a reminder.

Step 4: A second telephone call as a reminder.

The survey was carried out as a cross-sectional survey where data will be collected at one point in time. The form of data collection is regarded as a self-administered questionnaire. Selection of the respondents is chosen based on their convenience and availability, see also chapter 3.2.2. The survey instrument used in the thesis will be a self developed questionnaire containing all the three main aspects: consequences, handling/statistical regarding security breaches and ISMS implementation.

3.1.2 Validity and reliability of the method chosen

There will be three traditional forms of validity to look for, according to [17] p.157. Content validity, predictive or concurrent validity and construct validity.

Content validity:

Does the questionnaire measure what it was intended to measure? We think that the questionnaire measures what it was intended to measure the: consequences, handling security breaches, statistics about security breaches and the implementation of the ISMS in the organisations.

As mention in chapter 3.1 “Choice of method”, we discussed alternative and more extensive methods to collect data, but with the time and resources available in mind, we turned down all the alternatives apart from the questionnaire. These other methods may have given more exact data but there will be no guarantee. The respondents, independent of the method we select, may give us misleading data. Even if the method selected is in the form of an interview, an inspection or a document review, the respondents may give us misleading information.

The questionnaire contains both questions regarding qualitative and quantitative measures. We have tried to construct the questionnaire in such a way that, more than one question on each subject, will give us enough information to disclose misleading information

Predictive or concurrent validity:

Do the scores predict a criterion measures? Do results correlate with other results?

Construct validity:

Do the questionnaire measures hypothetical constructs or concepts? The questionnaire will not measure any hypothetical constructs or concepts. It will be a combination of:

- A range of closed-ended questions of the type “Yes” or “No” or a range of predefined answers
- Open-ended questions

Validity regarding the instrument (questionnaire) development:

We decided to execute a pilot survey before the questionnaire was send to all the respondents, see chapter 3.2.1 “Gained experience from pilot survey” for more information.

Data transformation:

Qualitative and quantitative data from the ISMS implementation in the organisations will be analysed and transformed to a quantitative measure of the maturity of the organisation.

Reliability:

How reproducible are the measurements? Our opinion is that the measurements are fairly reproducible. If someone else would execute a similar survey towards the respondents we believe that they will get nearly the same answers as we got. Improvements if the questionnaire is of course not taken into consideration. If any random errors are introduced into the survey we will hopefully be able to reveal them by our combination of questions. The margin of errors when mapping the answers to a predefined IS maturity scale is relatively high for the individual question. If the respondents deliberately give us incorrect answers for many questions, we will still be able to reveal the “wrong” answers. “Wrong” answers may be revealed when the maturity level shall be estimated.

3.2 Questionnaire

The questionnaire was developed in the period from February to the end of March. The pilot survey was performed in first half of April. The survey was performed in the second half part of April until the middle of May.

3.2.1 Gained experience from pilot survey

A preliminary version of the survey was distributed by email to two information security managers and one colleague at the master study. The information security manager represents two medium to large organisations in Norway. The pilot survey was performed in the middle of April.

The email contained detailed information about how it was planned to carry out the study. Forty Norwegian organisations would be asked to participate in the survey. The participants would receive an accompanying letter, the questionnaire, a letter of recommendation from the Norwegian Ministry of Trade and Industry and a prepaid return envelope. Information security manager or information security staffs within the organisations were the target for the questionnaire. In the pilot survey the participants were asked to take a critical look at the accompanying letter and the questionnaire. Is something in the questionnaire difficult to comprehend? Will it take too much time to answer the questions? Are the alternatives for the answers sufficiently adequate or are they too few? Do you think the organisation will have objections to answering the questions? And so on.

The feedback from the participants in the pilot-survey was very valuable. Eight changes were made to the questions. Some of the changes were comprehensive, while others were minor. One question was extensively restructured. In addition, an explanation was added to some of the special expressions. The accompanying letter was also improved according to the feedback in the pilot survey. Anonymity for the participating organisations was valued as very important. Without anonymity, several organisations would have difficulties in participating in the survey.

3.2.2 Selection of organisations from private sector and public sector

All organisations that were certified according to BS 7799-2 in Norway in April 2004 were a target for the questionnaire. In April 2004, there were nine organisations [3, 14] that were BS-7799-2 certified.

In addition, organisations which were expected to have implemented an ISMS were selected. Another reason for the selection was that the author has a professional relationship to the IS manager/staff in some of those organisations. In every organisation that was selected, we had a clear expectation that focus on IS was an important issue.

3.2.3 The questionnaire

The questionnaire was originally written in Norwegian and distributed to organisations in Norway. Appendix E contains the questionnaire translated from Norwegian to English. The intentions with the questions are explained in the appendix. The Norwegian version has precedence versus the following version in English.

Appendix C, contains the questionnaire in Norwegian.

3.3 Carrying out the survey

The survey was performed in the months April and May. A final version of the questionnaire (Appendix C) was ready in week 16 together with an accompanying letter (Appendix A) and a recommendation letter from the Norwegian Ministry of Trade and Industry (Appendix B).

When the survey foundation was ready we telephoned all security managers or information security staff in the 40 organisations which were selected. See chapter 3.2.2 for more information about the selection of organisations. The first call was made on 16th April and the last call was made on 5th May. Only one of the forty organisations was negative to contributing to the survey. The questionnaire, accompanying letter, recommendation letter and a reply envelope with postage stamp and date were distributed to 33 organisations on 20th April. The survey material was distributed to the remaining seven organisations on 22nd April. The replay envelope was to retain necessary anonymity.

In the period from 27th April to 5th May it was necessary to make reminder calls to all the organisations because we did not know which of the forty organisations that had returned the questionnaire, therefore we had to call all of them. We had to re-send the survey package to a few organisations. The deadline for returning the questionnaire was originally set to 27th April. The first questionnaire was received on 23rd April and the last on 18th May.

4. Results

A declared objective regarding this thesis was to guarantee anonymity of the participants. It should not be possible to trace the result in this report back to the organisations that participated in the survey.

On 18th May we have received 28 replies, which give a response rate of 70%. Two organisations have notified us that they unfortunately could not respond to the survey, but ten are still missing. We are satisfied with a response rate of 70%. Some of the honour, regarding the response rate, must be dedicated to the Norwegian Ministry of Trade and Industry for its contribution with the letter of recommendation.

4.1 General information and statistic from the survey

The following sub chapters contain general information and statistics regarding the main activity and the number of employees of the organisations.

4.1.1 The main activity in the participating organisation

The following figure gives an overview of the participating organisations regarding main activity. As mention before in the report, SIS in Norway [8] has divided all business and government activity into 11 categories. The 11 categories include “others”.

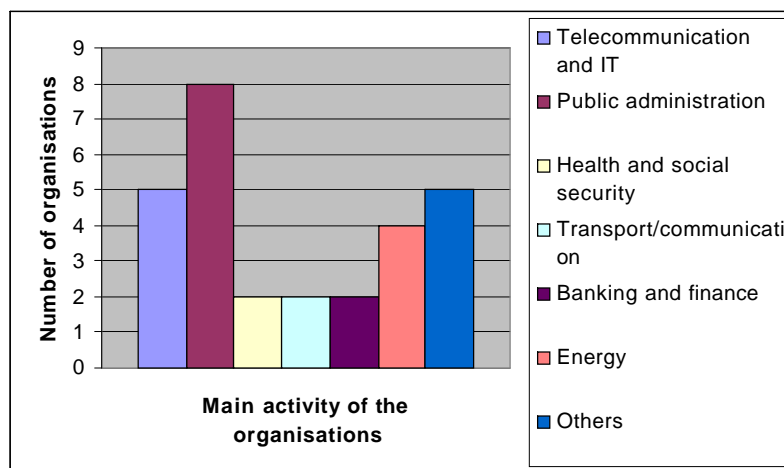


Figure 8: Main activity in the participating organisations

The following business sectors are not represented in the survey:

- Oil and gas
- Media and press
- Police and rescue service
- Research and education.

The nine organisations which are certified in Norway may be grouped into the following categories:

- Telecommunication and IT: 6
- Public administration: 1
- Banking and finance: 1
- Others: 1

Three of the certified organisations are of small to medium size within IS consultancy. These three organisations are categorised as “Telecommunication and IT”. As we can assume from the next chapter, 4.1.2 Distribution regarding the number of employees, none of these three organisations have participated in the survey. The reason is quite obvious for one of the organisations. The author is employed in one of them, VincIT AS.

4.1.2 Distribution regarding the number of employees

The numbers of employees in the participating organisations are presented in the following figure.

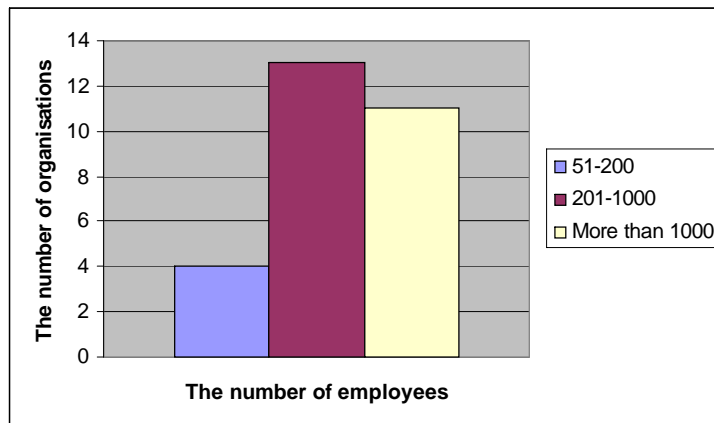


Figure 9: The number of employees in the organisations

All of the participating organisations have more than 51 employees and 86% of these organisations have more than 201 employees.

4.2 The distribution of ISMS in use

The following figure contains information about what kind of ISMS is in use in the participating organisations.

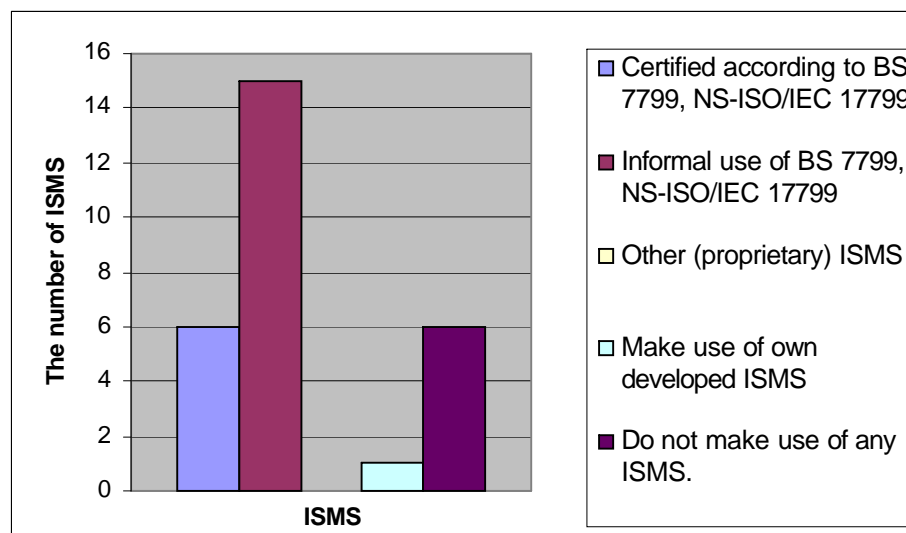


Figure 10: The distribution of ISMS

None of the participating organisations has implemented a type of proprietary ISMS.

Six organisations are certified according to the part 2 of the standard [4] and 15 organisations use the standard informally [13]. One organisation has developed their own ISMS and six of the organisations do not have an ISMS at all.

One of the six organisations that did not make use of any ISMS has more than 1000 employees and 4 of them have between 201-1000 employees.

4.3 IS resources in use and resources in use on preventive measures

Figure 11 shows how many man-labour years are used on IS and how many employees participate in IS tasks.

The checkboxes have the following range: 0-1, 2-4, 5-10, 11-20, 21-50 and above 50. We have also added those who did not answer the question, denoted as “blank”.

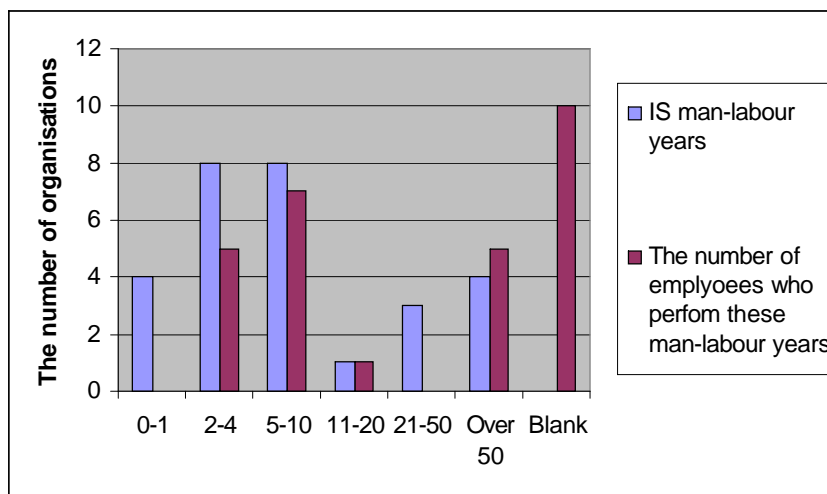


Figure 11: IS resources in use.

The organisations were asked how much effort was used on preventive measures in percent of the total resources that were used on the IS measures prevention, detection and reaction.

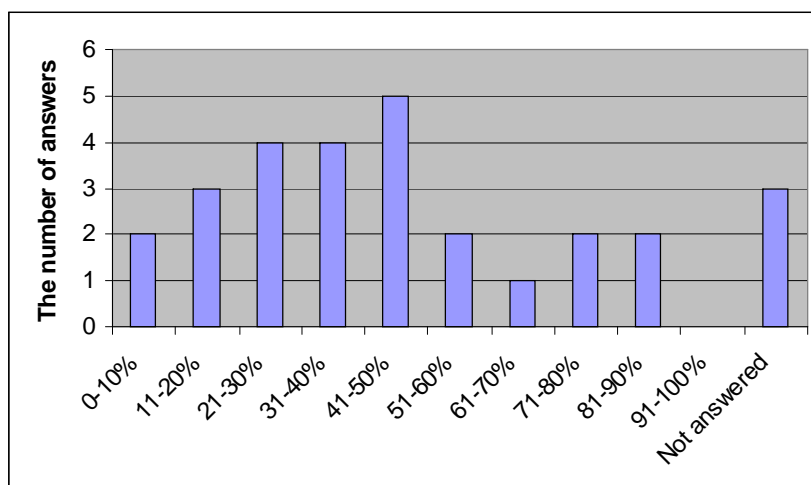


Figure 12: IS resources in use on preventive measures as a percent of the total resources in use.

As we see, resources used on preventive measures fluctuate between 0-10% and 81-90%.

4.4 IS policy in the organisations

We asked whether the organisations had a written IS policy. 24 of the 28 organisations in the survey had a written IS policy and 4 did not. Then we asked whether the IS policy was revised during the 12 last months. Seventeen of the organisations answered yes and 11 answered no. In other words 7 of the organisations with a written IS policy did not perform any revision during the last 12 months.

4.5 Management forum for IS

Fourteen organisations have established a management forum for IS. In 12 of these, the responsibility and tasks of the IS management forums were clearly defined. There were only 2 organisations where the management forum's responsibility and tasks were partly defined.

Fourteen organisations had not established any management forum at all.

4.6 Awareness

The first question we asked was whether any IS awareness campaigns or training were carried out during the last 12 months. Twenty-one of the organisations had performed campaigns or training during the last 12 months to all or some of the employees and hired personnel. In addition, 3 organisations had carried out IS awareness activities before the last 12 month period.

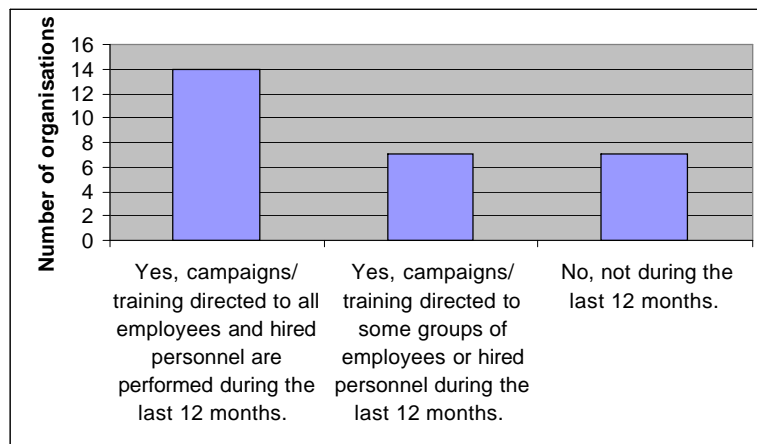


Figure 13: IS Awareness campaigns and training

The following types of IS awareness campaigns and training were carried out:

Posters, conferences, articles, skilled seminars, Intranet, internal newspapers, letters, emergency exercise, management crisis training, electronical programs, risk analysis, prevention of theft, use of password, handling of visitors, introduction course.

4.7 Risk analysis

Risk analyses had been carried out in 24 of the organisations. Figure 14 gives an overview of the reasons for carrying out risk analyses in the organisations.

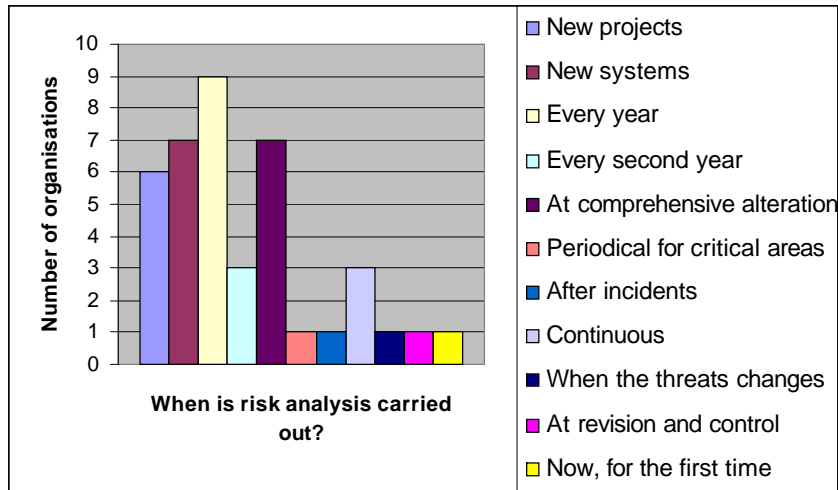


Figure 14: When is risk analysis carried out?

From the figure we see that the main reasons for carrying out risk analyses are the introduction of new projects and systems and when comprehensive alterations to systems have to be carried out. We also see that 9 organisations perform a risk analysis every year as a minimum and 3 do it every second year. Three organisations perform risk analysis continuously.

The following methods and tools are used to carry out risk analyses: self-developed method, risk assessment, Telerisk, simplified risk assessment, check lists, HASOP, guideline from the Norwegian Directorate for Civil Protection and Emergency Planning, CRAMM, SARA and SPRINT from ISF, SBA, NS/ISO 5814, NS-ISO/IEC 17799, guideline from the Data Inspectorate in Norway, help from external consultants and mapping of vulnerabilities and critical factors.

Only self-developed methods, Telerisk and NS 17799 were mentioned more than once. "Self-developed methods" was mentioned more often than anything else.

Nearly one half of the organisations gave a useful answer to question 19. We asked whether it was possible to state the formula that was in use for calculation of the risk. None of the formulas were pointed out more than once. The formulas mentioned are to be found in appendix D.

4.8 Business continuity management

The following figure shows the results from question no. 24 regarding business continuity management.

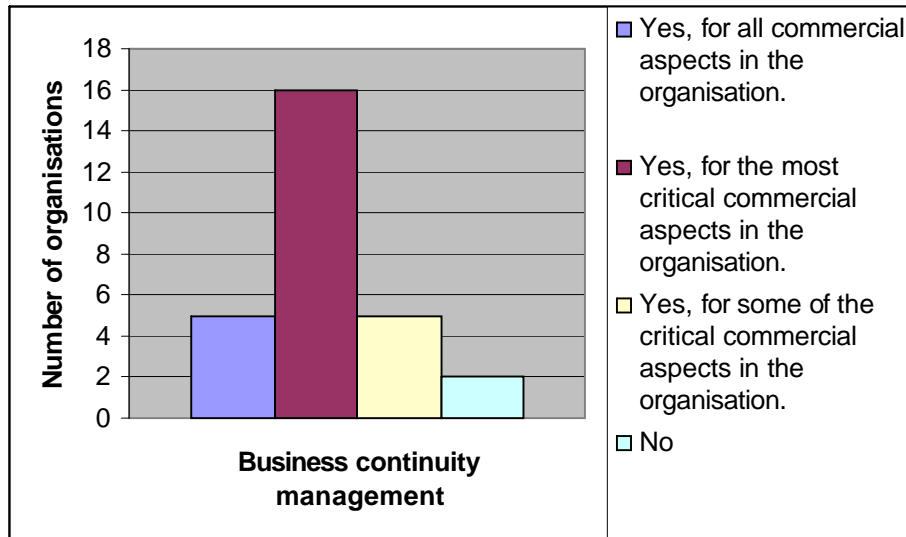


Figure 15: Business continuity management in the organisations

All organisations apart from 2 have established processes for the development and maintenance of the business continuity management.

Table 4: Which elements is a part of the business continuity management process?

Question #25	Question	Yes	No
B	Risk analysis, including the likelihood and the impact of possible security incidents.	18	10
C	Identification and prioritization of critical business processes.	20	8
D	An overview and understanding of the impact which interruptions are likely to have on the business.	17	11
E	Possible insurance scheme is considered as a part of the continuity management strategy.	6	22
F	A documented business continuity strategy is worked out.	10	18
G	Business continuity plans, disaster recovery plans and crisis management plans are worked out according to approved strategy.	19	9
H	The plans are tested at regular intervals.	13	15
K	The plans are updated at regular intervals.	17	11
M	The responsibility for co-ordinating the business continuity management process is assigned.	18	10

Table 4 is a collection of the questions with the “Yes” and “No” alternatives. As we see, adding the amount of “Yes” and “No” answers gives us 28. Those respondents that have not answered these questions are all interpreted as “No”.

Question E regarding insurance scheme has got a very low score. Only 6 out of 28 organisations look at the insurance scheme as a part of the business continuity management process. Question F, regarding a documented business continuity strategy has also obtained a low score.

Questions B, C, D, G, K and M have all obtained a high score. Risk analysis, identification and prioritization of critical business processes, understanding the impact, worked out plans, updating the plans and the responsibility for co-ordinating the business continuity management process is assigned are elements in the business continuity management process in many of the organisations.

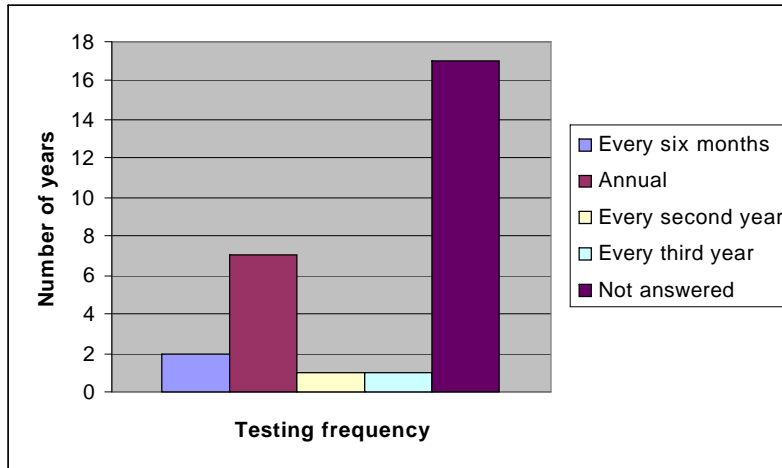


Figure 16: Question 25i, testing frequency

The answers regarding the testing frequency are disappointing. Only 9 organisations have answered this question. A good practice is to test the plan as a minimum annually. Seventeen organisations have not answered this question.

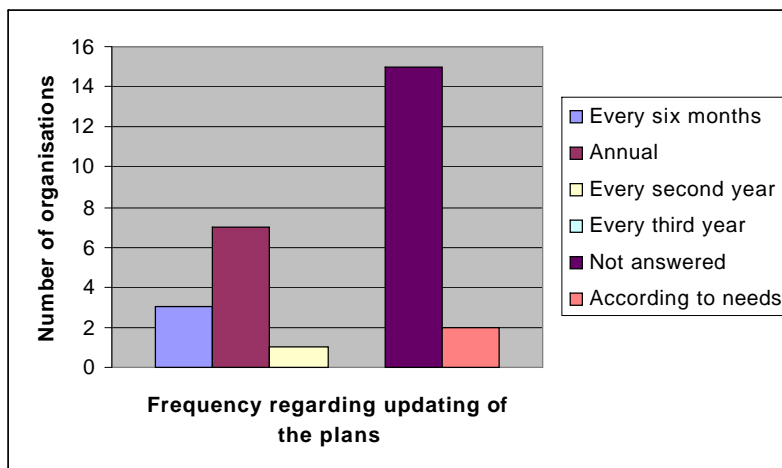


Figure 17: Question 25l, updating frequency

The answers regarding the updating frequency are a little positive than testing frequency. Eleven organisations are updating the plans at least every second year and in addition 2 organisations do it according to needs. A good practice is to update the plan as a minimum annually. Fifteen organisations have not answered this question.

4.9 IS breaches and statistics in the organisations

The following Figure 18: Statistical register regarding security breaches, contains the results from question #26. Will actual security breaches and attempt on security breaches be registered in a statistical register?

Organisations which have matured ISMSs should also have control regarding actual security breaches and security breaches attempt. A perfect result from the survey would be as follows. Enough organisations which have control regarding actual security breaches and are able to detect attempt on security braches. Further, they are able to maintain continuous statistical records. If this is the situation it will be possible to compare the kind of ISMS, the year when the ISMS was implemented and the statistical records regarding security breaches.

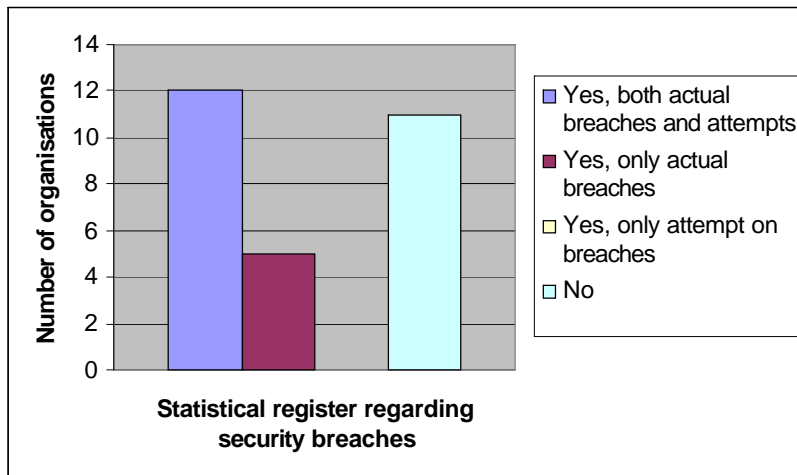


Figure 18: Statistical register regarding security breaches

Twelve organisations have a statistical register concerning both actual security breaches and attempts. Five organisations have statistical register concerning only actual breaches.

Question #27: 15 organisations have statistics for the previous years. The answers are illustrated in Table 5.

Table 5: Statistics for security breaches in the organisations, retrospective in years

	1 year	2 years	3 years	4 years
Number of organisations	2	5	4	4

Not every one of those who answered question #26 positively have answered question #27. We see from Table 5 that 13 organisations have statistical data for more than 2 years and 4 organisations 4 years. No one has statistical data for more than 4 years. If we going 4 years back in time we will end up in the year 2000. This start regarding registration of statistical data may be as a result from work in connection with Y2K.

4.10 Handling security breaches - incident response team

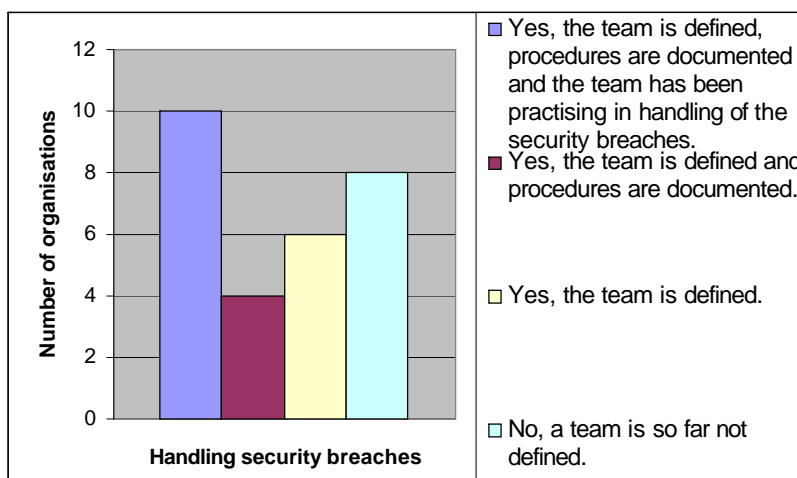


Figure 19: Handling security breaches in the organisations

A kind of incident response team is established in 20 organisations, however only 10 organisations have documented the procedures and executed training regarding handling security breaches.

Table 6: Team to handle security breaches - numbered years in existence

	1 year	2 years	3 years	4 years	More than 10 years
Number of organisations	3	5	2	6	2

Eighteen of the organisations answered this question and in 8 organisations the team has existed in more than 4 years. In 2 organisations the team has been established for more than 10 years.

4.11 Consequences in the organisations

Figure 20 gives an overview of the consequences which have hit the organisations since 1999.

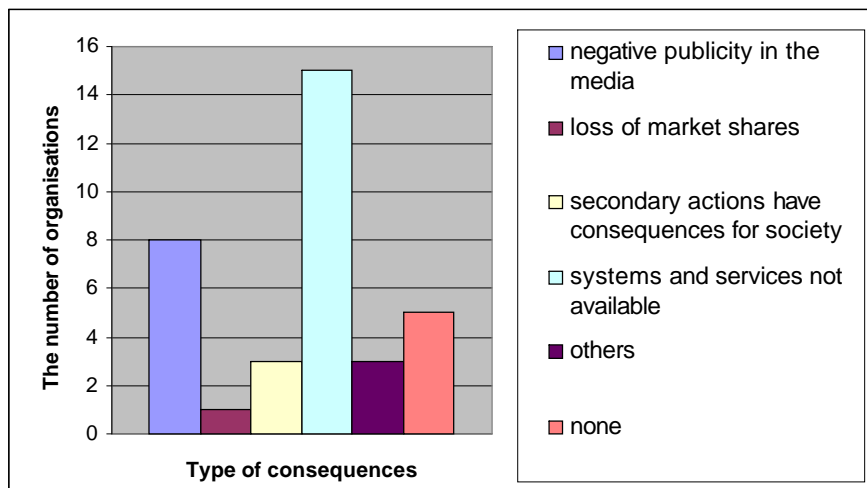


Figure 20: Actual consequences experienced by the organisations

Each organisation did have the possibility to mark more than one consequence. 3 of the 28 organisations that have taken part in the survey did not give any answer to this question. As Figure 20 shows, there have not been any loss of life and only 1 organisation has experienced loss of market shares. More than half of the organisations reports missing availability of systems and services as the most general consequence. Eight of the organisations have experienced negative publicity in the media. Five organisations have not experienced any consequences in the last 6 years. Totally, 30 consequences are reported in the survey.

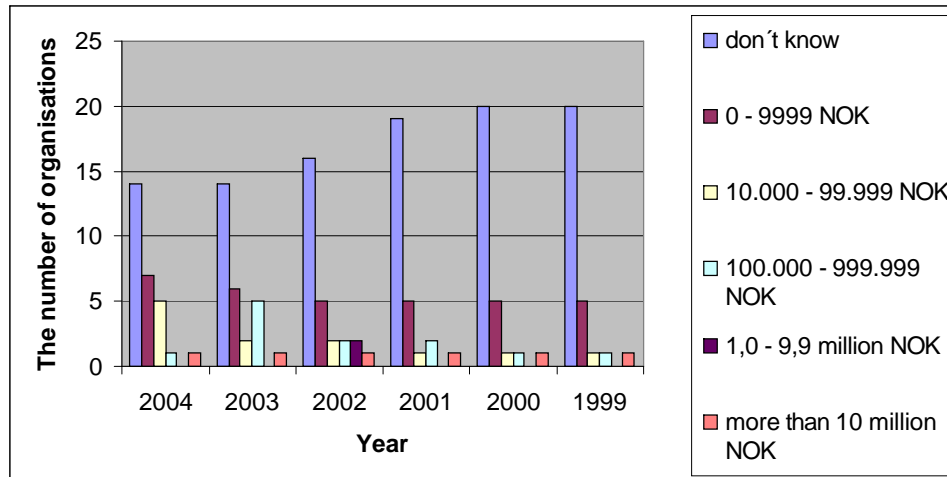


Figure 21: The actual consequences estimated as financial loss

Three of those 5 respondents that answered “none” in question 32, regarding consequences, have not answered question 33. Those 3 respondents, #1, #7 and #20, have been adjusted to 0 - 9999 NOK in annual loss for the years 1999 to 2004. “None” should of course have been an alternative in question 32.

Two of the respondents, # 16 and #25, had not marked anything in question 32 or in 33. For those 2 respondents, question 33 is recorded as “don’t know” regarding annual loss.

Figure 21 gives an overview of actual consequences as financial loss for the organisations. After necessary adjustment of the respondents’ answers, we find that only 8 organisations have completed this question regarding the estimation of financial loss for the actual period. One of these organisations has answered more than 10 million NOK for all these years. Seven organisations have answered this question for some of the years and as many as 13 organisations are not able to estimate the consequences as financial loss at all. 54% of the 28 organisations in this survey have been able to estimate consequences as financial loss for the whole period or parts of the period.

Seventeen organisations have experienced consequences in the period 1999-2004, but only 10 (59%) of these are able to estimate the consequences in financial loss.

Four out of 6 certified organisations are not able to estimate the consequences as financial loss. This result is very astonishing and was not what we expected to find.

4.12 Determination of the organisations ISMS maturity level

In appendix E the questionnaire is translated into English with an explanation and intentions with the questions. For every question we have added a section “Input to thesis”. In this section we have placed vital information on how to interpret the answers and particularly how to interpret the answers regarding the maturity level of the organisations.

A spreadsheet is used to gather all the replies and appendix D contains an extract of the spreadsheet.

The maturity of organisations is described in chapter 2.3. With reference to Table 1: Maturity of information risk management [1, 26], on page 16, and Appendix D, we have analysed the questionnaire replies from the organisations and assigned a maturity level to each one. About 6 of the replies were on the borderline regarding which maturity level they belonged to. Minor changes in the organisation may lead to a higher or lower maturity level.

The following table shows the resulting ISMS maturity level.

Table 7: The organisations ISMS maturity level

Questionnaire reply	The kind of ISMS in use	Maturity level
#1	Certified according to BS 7799	2
#2	Informal use of BS 7799	1
#3	Certified according to BS 7799	3
#4	Informal use of BS 7799	3
#5	Certified according to BS 7799	3
#6	Informal use of BS 7799	1
#7	Informal use of BS 7799	1
#8	Informal use of BS 7799	2
#9	Own developed ISMS	2
#10	Do not make use of any ISMS	1
#11	Informal use of BS 7799	2
#12	Informal use of BS 7799	1
#13	Do not make use of any ISMS	1
#14	Informal use of BS 7799	1
#15	Informal use of BS 7799	1
#16	Certified according to BS 7799	2
#17	Informal use of BS 7799	2
#18	Do not make use of any ISMS	0
#19	Informal use of BS 7799	1
#20	Informal use of BS 7799	1
#21	Informal use of BS 7799	1
#22	Do not make use of any ISMS	0
#23	Do not make use of any ISMS	0
#24	Informal use of BS 7799	2
#25	Certified according to BS 7799	2
#26	Certified according to BS 7799	2
#27	Informal use of BS 7799	2
#28	Do not make use of any ISMS	0

According to Fung, Farn and Lin [1] BS 7799-2 certified organisations should belong to maturity level 3 and above. As we see from Table 7, we could only place 2 out of 6 certified organisations into maturity level 3.

The following table shows the numbers of organisations in each maturity level.

Table 8: Number of organisations within each type of ISMS and maturity level

	M-level 0 Non-existent	M-level 1 Initial/Ad-Hoc	M-level 2 Repeatable but intuitive	M-level 3 Defined process
Certified according to BS 7799			4	2
Informal use of BS 7799		9	5	1
Own developed ISMS			1	
Do not make use of any ISMS	4	2		

4.13 Statistical estimates

Bootstrap is a computer-based method for assigning measures of accuracy to statistical estimates [2], which can be used to produce inferences.

In the bootstrap method is about drawing and then put it back, resampling, from a small amount of data. After completion we get a new sample called the bootstrapping sample, which is considered to be independent of the original data. The statistical properties of the new data can be used to examine the properties of the initial data.

In the three following chapters we have used the application “R”, Windows version (95 and later), downloaded from the R-projects website [29]. A program had to be developed in “R” to calculate the statistical values depending on the replies from the questionnaire.

One organisation uses its own developed ISMS. It is not possible to use the bootstrap method because of too few occurrences.

The bootstrap calculations are given with 1 digit in the decimal. We are aware that the methods used in the questionnaire lead to using maximum one digit in the decimal. One digit may also be too much but, in spite of this, the bootstrap method is used to demonstrate how to get a sufficient statistical amount of data from a small amount of data.

With 1000 bootstrap values we received the following results.

4.13.1 Bootstrap - estimation of average for certified organisations

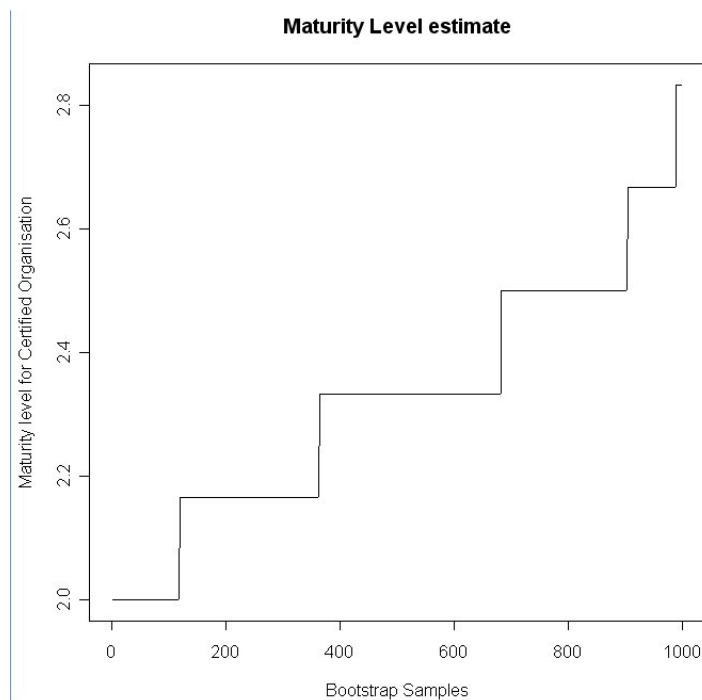


Figure 22: Maturity level for certified organisations

The average estimate for organisations which are certified according to BS 7799 is 2.3 and the 5%-95% area of the values are between 2.0 - 2.7. The standard error of mean in the originally data set is calculated to 0.21 and to 0.19 in the bootstrap data set. See appendix F for the program details.

4.13.2 Bootstrap - estimation of average for informal use of the standard

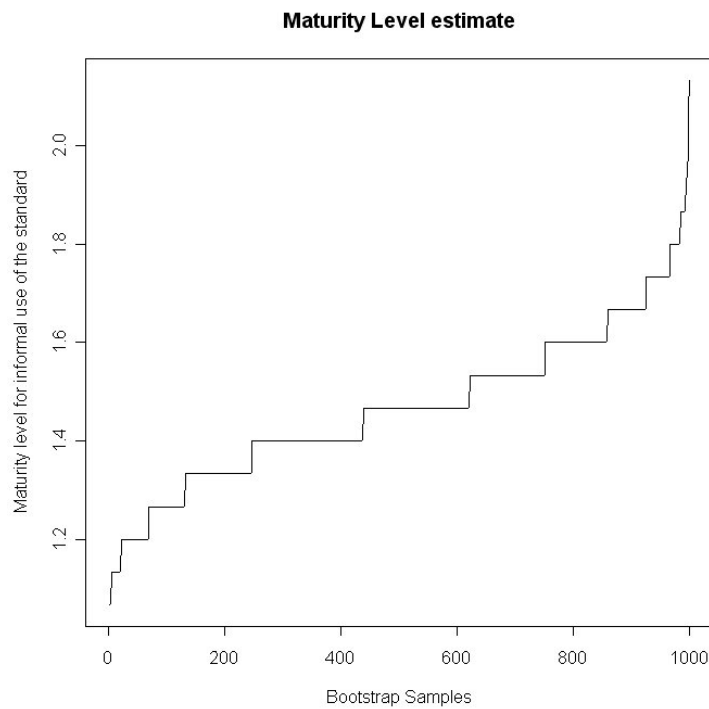


Figure 23: Maturity level for the informal use of the standard

The average estimate for organisations which use the standard in an informal way is 1.5 and the 5%-95% area of the values are between 1.1 - 1.8. The standard error of mean in the original data set is calculated to 0.16 and to 0.16 in the bootstrap data set. See appendix F for the program details.

4.13.3 Bootstrap - estimation of average for organisations that do not use any standard

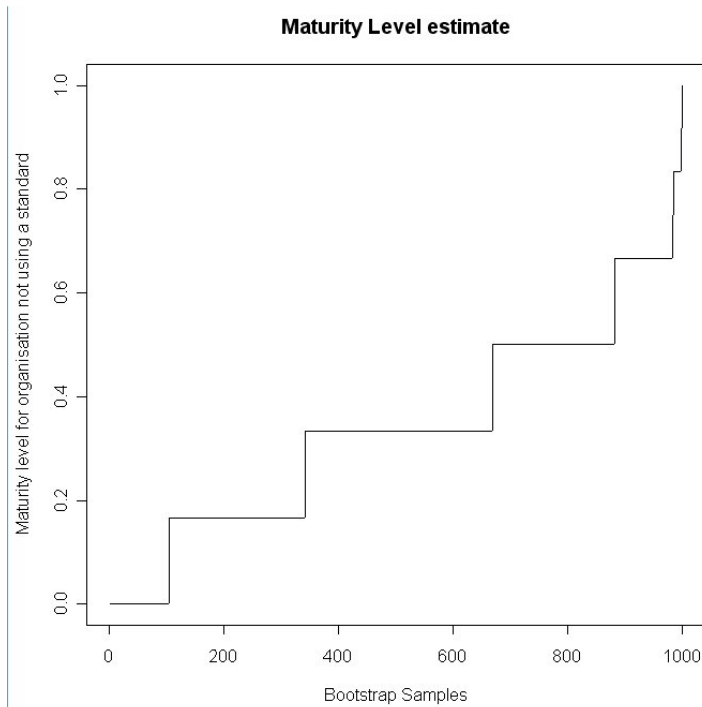


Figure 24: Maturity level for organisations which do not use any standard

The average estimate for organisations that do not use a standard is 0.3 and the 5%-95% area of the values are between 0.0 - 0.7. The standard error of mean in the original data set is calculated to 0.21 and to 0.18 in the bootstrap data set. See appendix F for the program details.

4.13.4 Boxplot

A boxplot is a way to look at the overall shape of a set of data. The box shows the data between the “hinges”, with the median represented by a line. “Whiskers” go out to the extreme of the data, and very extreme points are shown by themselves.

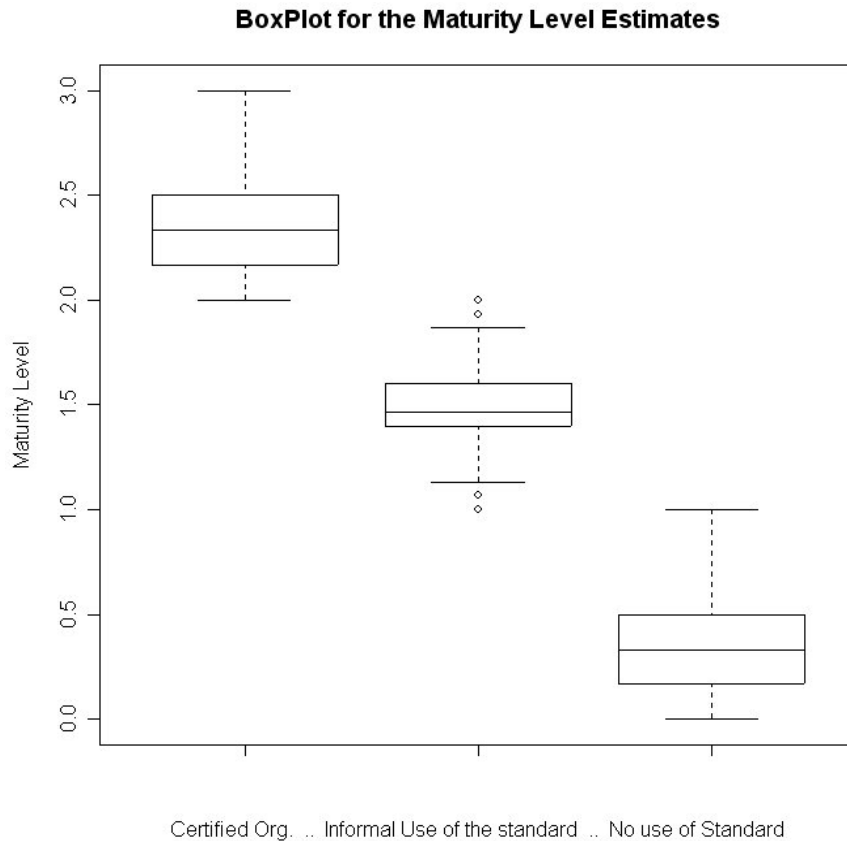


Figure 25: An overall shape of the bootstrap data

The “hinges” in this boxplot shows the 25-75% of the data.

See appendix F for the “R” command details.

5. Discussion

In chapter 3.1 Choice of method we have described the construction of the questionnaire.

The questionnaire was constructed to contain the following three main IS aspects:

- the **consequences of security breaches** which have hit the organisations from 1999 to 2004, estimated as financial loss
- how security breaches are handled in the organisation and the possibilities for us to get access to **statistical data regarding security breaches**
- which parts of the ISMS are implemented and how they are implemented to measure the **maturity** of the ISMS.

Consequences of security breaches:

Figure 21, at page 34, gives an overview of actual consequences as financial loss for the organisations. After necessary adjustment of the respondents' answers, we find that only 8 organisations have completed this question regarding the estimation of financial loss for the actual period. One of these organisations has answered more than 10 million NOK for all these years. Seven organisations have answered this question for some of the years and as many as 13 organisations are not able to estimate the consequences as financial loss at all. 54% of the 28 organisations in this survey have been able to estimate consequences as financial loss for the whole period or parts of the period.

Seventeen organisations have experienced consequences in the period 1999-2004, but only 10 (59%) of these are able to estimate the consequences in financial loss.

Four out of 6 certified organisations are not able to estimate the consequences as financial loss. This result regarding certified organisations was very astonishing and was not what we expected to find.

The statistical data regarding consequences of security breaches was too small to perform any statistical analysis.

Statistical data regarding security breaches:

Twelve of the organisations have a statistical register concerning both actual security breaches and attempts. Further, five organisations have statistical register concerning only actual breaches.

Thirteen organisations have statistical data for more than 2 years and 4 organisations 4 years. No one has statistical data for more than 4 years.

Our last question was whether the organisations could place statistics/documentation to disposal. Necessary "washing" of the statistics/documentation has to be done before handover.

The access to statistical data regarding security breaches was too small to perform any statistical analysis.

ISMS Maturity:

In appendix E the questionnaire was translated into English with an explanation and intentions with the questions. For every question we have added a section "Input to thesis". "Input to thesis" is vital information on how to interpret the answers and particularly how to interpret the answers regarding the maturity level of the organisations.

The replies and "Input to thesis" sections are analysed towards the ISMS maturity classification in Table 1: Maturity of information risk management [1, 26], on page 16. An ISMS maturity level is assigned to the replies from each organisation.

In Table 8: Number of organisations within each type of ISMS and maturity level, at page 35, we presented an overview of the maturity level of the organisations.

Table 8 is extended with the average maturity level within each ISMS category of organisations. The result is presented in Table 9. The average maturity level for each ISMS category is calculated as follows:

Formula: (Organisation #A + Organisation #B +..... + Organisation #N) / N = Average maturity level

Table 9: The mean maturity level of the organisations within each type of ISMS

	M-level 0 Non-existent	M-level 1 Initial/Ad-Hoc	M-level 2 Repeatable but intuitive	M-level 3 Defined process	Average maturity level
Certified according to BS 7799			4	2	2,3
Informal use of BS 7799		9	5	1	1,5
Own developed ISMS			1		2,0
Do not make use of any ISMS	4	2			0,3

The results from the survey show that the average maturity level for the organisations are as follows:

- certified organisations according to BS 7799-2, **2.3**
- informal use of the BS-7799 / ISO/IEC 17799 standards in the organisations, **1.5**
- for organisations that do not use a standard and have not implemented any ISMS, **0.3**

The boxplot diagram, Figure 25: An overall shape of the bootstrap data, at page 39, shows the results from using the bootstrap method on our data findings. Using 1000 bootstrap values we got the results presented in Figure 25.

The figure shows the data between the “hinges”, with the median represented by a line. “Whiskers” go out to the extreme of the data, and very extreme points are shown by themselves. The “hinges” in this boxplot shows the 25-75% of the data.

We see that there is a distinct distribution of the plots regarding the three ISMS categories. We think that the distributions in the boxplot diagram emphasise our findings.

There is a significant difference between these three levels of implementing or not implementing an ISMS. We have been very cautious when we have decided the maturity level in the certified organisations. According to Fung, Farn and Lin [1] BS 7799-2 certified organisations should belong to maturity level 3 and above. As we see from Table 7 we could only place 2 out of 6 certified organisations into maturity level 3.

The survey shows that organisations that have not implementing any ISMS are at **level 0 (Non-existent: management processes are not applied at all)**. Organisations that use the standard in an informal way, are at **level 1 (Initial/Ad-Hoc: processes are ad-hoc and disorganized)** and certified organisations are at **level 2 (Repeatable but intuitive: processes follow a regular pattern)**.

The results from the survey fit in with other research results regarding ISO 900x and ISMS maturity within organisations [1, 11, 16, 20, 23].

We have to remember that the questionnaires were answered by information security managers or information security staffs within the organisations and not by a broad group within the organisations. If we had unlimited resources available and no time limits, then we might have wanted to perform this survey in another way. We could have interviewed a broad group of employees and management regarding the IS challenge and maturity level. And in addition we could have performed many technical tests regarding IS. The tests could have been performed according to the Open-Source Security Testing Methodology Manual [25].

5.1 Practical problems

The development of the questionnaire took a great deal of time to complete and we should have had more focus on the analysing part. The questionnaire could have been more compact. Some of the questions were unnecessary and some questions were missing. A question about any quality certification was one that was missing. The questionnaire could also have been more directed to measuring the maturity of the organisations.

6. Conclusion and further work

Research presented in the articles [10, 16] supports our statement that the quality of IS within an organisation has a relation with the maturity level of the organisation.

Research regarding ISO 9000 [16] concludes that the value of implementing certification can be increased by identifying and introducing additional goals besides certification and enhancing the change process, sometimes by adding minor extra resources.

Paper regarding maturity of organisations [20] is based on participation at several workshops and site visits in thirteen software organisations at maturity level 4 and 5. Even if none of the respondents in our survey are at this maturity level we find the findings in the relevant for our thesis. Eleven of the organisations in the survey had ISO 9001 certification. Other characteristics of the organisations are that they emphasize openness, communication, and a commitment to quality and the customer at all levels. They encourage a process orientation in their staff and worker empowerment and participation in process definition and improvement activities are real; process improvement is part of everyone's job. It is also difficult to be a high maturity organisation, if you have low maturity customers, suppliers or partners.

Our opinion is that the survey, regarding the ISMS maturity, measures what it was intended to measure. The results are in accordance with other research in the field of ISO 900X and maturity of organisations [16, 20]. The results are also in accordance with common sense. When using common sense it is to expect that certified organisations, in mean, will obtain a higher ISMS maturity level. Which leads to a higher level regarding the IS status.

The validity of the data collected is regarded as expected according to chapter 3.1.2 Validity and reliability of the method chosen.

The pilot survey gained us experience of great value, but there is still possible to improve and increase the efficiency of the questionnaire.

Our opinion is also that the measurements are fairly reproducible and that the degree of reliability is satisfactory.

The conclusion in this thesis is that organisations certified according to BS 7799-2 have a higher maturity in the organisation versus organisations that have chosen to only use the standard in an informal way. Those organisations that use the standard informally have higher maturity than those organisations that do not implement any ISMS.

We believe that our findings support the statement. BS 7799 will be worth the effort for organisations which needs to protect their assets.

6.1 Further work

As mention in chapter 5, if we had unlimited resources available and no time limits then we might have wanted to perform this survey in another way. We could have interviewed a broad group of employees and management regarding the IS challenge and the maturity level combined with technical inspection and testing. We could also have performed remote testing regarding the IS.

Remote testing according to OSSTMM [25] could be reduced to test network surveying, port scanning and denial of service.

A questionnaire in the shape of an automated web-application with sufficient security could be of great help in collecting data from organisations worldwide. This technique in combination with cross

questions to disclose answers which contaminate the survey might lead to a data set from which it would be possible to perform a better statistical analysis.

A number of master students have in this semester performed master thesis as a survey where management has been an important part. The data collected in these thesis may be correlated and hopefully give us more valuable knowledge about the IS challenge.

7. References

- [1] A. Ren-Wei Fung, K. Farn, A.C. Lin. Paper: a study on the certification of the information security management systems. *Computer Standards & Interfaces* 25, 2003, pp. 447-461
- [2] B. Efron, R.J. Tibshirani. *An introduction to the Bootstrap*. Chapman & Hall/CRC, 1993. ISBN 0-412-04231-2
- [3] BizKit KvaLex. A Norwegian database regarding certified organisations. <http://www.kvalex.no> (accessed April 14, 2004)
- [4] British Standard. BS 7799-2:2002 Information security management systems - Specification with guidance for use. British Standards Institution. 2002
- [5] B. Solms, R. Solms. Incremental information security certification. *Computers and Security*, 20 (4), pp. 308-310, 2001.
- [6] Carnegie Mellon Software Engineering Institute. [Online] Available at <http://www.sei.cmu.edu/cmm/> (accessed May 10, 2004)
- [7] Carnegie Mellon Software Engineering Institute. [Online] Available at <http://www.sei.cmu.edu/cmm/cmm.sum.html> (accessed May 12, 2004)
- [8] Centre for Information Security (SIS). [Online] Available at http://www.norsis.no/rapportere_hendelse1.php (accessed May 20, 2004)
- [9] *COBIT 3rd Edition Management Guidelines*. COBIT Steering Committee and the IT Governance Institute, 2000
- [10] D. Osterwalder. Trust through evaluation and certification? *Social Science Computer Review*, vol. 19, no. 1, 2001, pp. 32 - 46
- [11] D. Stelzer, W. Mellis, G. Herzwurm. A critical look at ISO 9000 software quality management. *Software Quality Journal* 6, 1997, pp. 65 - 79
- [12] Gamma Secure Systems Limited. History of 7799. [Online] Available at <http://www.gammassl.co.uk/bs7799/history.html> (accessed May 10, 2004)
- [13] International Organisation for Standardization and International Electrotechnical Commission. ISO/IEC 17799:2000 Information technology - Code of practice for information security management. ISO/IEC 2000
- [14] ISMS International User Group. Certification register. [Online] Available at <http://www.xisec.com> (accessed 11. December 2003)
- [15] ISO, Information Technology - Guidelines for the Management of IT Security, Parts 1 - 5. ISO/IEC TR 13335 (All Parts), ISO (2001).
- [16] J. Karltn, J. Axelsson, J. Eklund. Working conditions and effect of ISO 9000 in six furniture-making companies: implementation and processes. *Applied Ergonomics*, vol. 29, no. 4, 1998, pp. 225 - 232
- [17] J.W. Creswell. *Research Design, Qualitative, Quantitative and Mixed Methods Approaches*. Sage Publications, 2002. ISBN 0761924426

- [18] M.C. Paulk, B. Curtis, M.B. Chrissis, C.V. Weber. Capability Maturity ModelSM for Software, Version 1.1. *Software Engineering Institute Carnegie Mellon University*, Technical Report CMU/SEI-93-TR-024,ESC-TR-93-177, 1993
- [19] M.C. Paulk, C.V. Weber, S.M. Garcia, M.B. Chrissis, M. Bush. Key Practices of the Capability Maturity ModelSM, *Software Engineering Institute Carnegie Mellon University*, Technical Report CMU/SEI-93-TR-025, ESC-TR-93-178. 1993.
- [20] M. C. Paulk. *Practices of High Maturity Organizations*. 1999 SEPG Conference, Atlanta, Georgia, 8-11 March 1999.
- [21] M.M. Eloff, S.H. von Solms. Information Security Management: An Approach to Combine Process Certification And Product Evaluation. *Computers & Security*, vol. 19, no. 8, 2000, pp. 698-709
- [22] M. Swanson, N. Bartol, J. Sabato, J. Hash, L. Graffo. *Security Metrics Guide for Information Technology Systems*. 2003, NIST Special Publication 800-55
- [23] M. Terziovski, D. Power, A.S. Sohal. The longitudinal effects of the ISO 9000 certification process on business performance. *European Journal of Operational Research* 146, 2002, pp. 580 - 595
- [24] OECD Guidelines for the Security of Information Systems and Networks Towards a Culture of Security. *OECD Science & Information Technology*, vol. 2002, no. 9, pp. 1-30
- [25] P. Herzog. *Open-Source Security Testing Methodology Manual version 2.1*. Institute For Security And Open Methodologies, August 23, 2003.
- [26] P.W. Andersen. Information Security Governance. *Information Security Technical Report*, vol. 6, no. 3, 2001, pp. 60-70
- [27] T. Daler, R. Gulbrandsen, T.A. Høie, B. Melgård, T. Sjølstad. *Handbook in data security* (Norwegian: *Håndbok i datasikkerhet*). Tapir akademisk forlag, 2002. ISBN 82-519-1785-9
- [28] *The Forum's Standard of Good Practice*. Information Security Forum, 2000
- [29] The R Project for Statistical Computing. [Online] Available at <http://cran.us.r-project.org/> (accessed May 16, 2004)
- [30] W. C. Booth, G. G. Colombs, J. M. Williams. *The Craft of Research*. The University of Chicago Press, 2003. ISBN 0-226-06568-5

Appendix A: Accompanying letter distributed with the questionnaire

Spørreundersøkelse - Mastergradstudier i informasjonssikkerhet ved Høgskolen i Gjøvik

Mitt navn er Frank-Arne Stamland og jeg gjennomfører en Masteroppgave i informasjonssikkerhet ved Høgskolen i Gjøvik. Min veileder er Professor Einar Snekkenes og mer informasjon om studiet og masteroppgaven er å finne på <http://www.nislab.no>. I tillegg til studiet arbeider jeg som aktiv partner i VincIT Risk Management AS.

Tema for oppgaven er å måle eventuelle effekter av et ledelsessystem/styringssystem for informasjonssikkerhet. Vedlagt følger et spørreskjema som jeg ønsker at du besvarer på vegne av virksomheten. Undersøkelsen er forventet å ta 15 - 30 minutter.

Det vil bety mye for meg om du kan avsette nødvendig tid for å besvare spørreskjemaet. Et anbefalingsskriv fra Nærings- og handelsdepartementet ved avdeling for IT-politikk er vedlagt for å understreke viktigheten av spørreundersøkelsen.

Så langt har det vært gjennomført lite forskning innenfor dette området. Det finnes ingen direkte vitenskapelige undersøkelser eller litteratur som bekrefter eller avkrefter effekten av å etablere denne typen ledelsessystemer. Hensikten med spørreundersøkelsen er å få tilstrekkelig med underlag i form av besvarelser, slik at det vil være mulig å bekrefte eller avkrefte effekten av et ledelsessystem/styringssystem for informasjonssikkerhet.

Spørreskjemaet er sendt til ca. 30 norske private og offentlige virksomheter. Spørsmålene ønskes besvart ved at du krysser av i sjekkbokser eller skriver svarene direkte i fritekstdelen av spørreskjemaet. Benytt eventuelt baksiden av arkene hvis det er for liten plass.

Vedlagt følger en ferdig frankert konvolutt for retur av spørreskjemaet. Virksomhetens medvirkning og besvarelse vil forbli anonym og besvarelsen vil bli håndtert med nødvendig konfidensialitet.

Alle virksomhetene som har vært med i undersøkelsen vil få en kopi av rapporten. På forhånd takk for at dere tok dere tid til å være med på undersøkelsen!

Jeg vil sette pris på om spørreskjemaet kan returneres så raskt som mulig og helst innen 27. april.

Med vennlig hilsen

Frank-Arne Stamland
Mastergradsstudent informasjonssikkerhet
Høgskolen i Gjøvik

Ved eventuelle spørsmål eller behov for avklaringer vil jeg være å treffe på følgende telefonnummer: Kontor 35 57 41 38, Mobil 90 57 67 57, alternativt på følgende e-post: frank-arne.stamland@vincit.no

Appendix B: Letter of recommendation from the Norwegian Ministry of Trade and Industry



DET KONGELIGE
NÆRINGS- OG HANDELSDEPARTEMENT

Til virksomheten

Deres ref

Vår ref

Dato
15.04.2004

Oppgave på mastergradsnivå innen informasjonssikkerhet.

Mastergradsstudiet innenfor informasjonssikkerhet ble etablert ved Høgskolen i Gjøvik høsten 2002, med støtte av bl.a. Nærings- og handelsdepartementet, Telenor, Forsvaret mfl.

Etableringen av studiet er et ledd i gjennomføringen av en Nasjonal strategi for informasjonssikkerhet, vedtatt av regjeringen i mai 2003. Strategien kan leses i sin helhet på adressen <http://odin.dep.no/archive/nhdvedlegg/01/06/Nasjo006.pdf>.

Økt kompetanse om informasjonssikkerhet i hele samfunnet er en prioritert målsetting i strategien, som også omfatter tiltak rettet bl.a. mot økt bevisstgjøring av virksomheter og husholdninger når det gjelder utfordringer knyttet til IT-sikkerhet og sikker bruk av Internett.

Etablering av en policy for informasjonssikkerhet, iverksetting av gode sikkerhetsrutiner, og utvikling av kompetanse om informasjonssikkerhet blant ansatte i norske bedrifter er et viktig element i realiseringen av en "kultur for sikkerhet" som strategien er tuftet på.

For å kunne finne frem til relevante sentrale tiltak på dette området, og dermed hjelpe næringslivet i å etablere en slik kultur for sikkerhet, trenger vi imidlertid dybdekunnskap om tilstanden innen dette feltet i norske bedrifter. Vi vil derfor anbefale sterkt at bedriften bidrar til dette gjennom å besvare den vedlagte henvendelsen fra Frank Arne Stamland ved Høgskolen i Gjøvik. Kunnskapen som denne undersøkelsen kan gi vil kunne brukes til å utvikle relevante anbefalinger og metoder som kan bidra til

Postadresse
Postboks 8014 Dep
0030 Oslo

Kontoradresse
Einar Gerhardsens plass 1

Telefon
22 24 90 90
Org no.
972 417 890

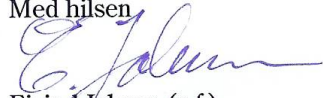
Avdeling for IT-politikk
Telefaks
22 24 03 15

Saksbehandler
Katarina de Brisis
22 24 67 30

styrking av IT-sikkerheten i næringslivet, og gjennom erfaringsoverføring, i samfunnet for øvrig.

Vi takker for deres ev. bidrag og ser frem til resultater fra undersøkelsen, som vi regner med vil bli tilgjengeliggjort for alle deltakere.

Med hilsen



Eivind Jahren (e.f.)
avdelingsdirektør



Katarina de Brisis
seniorrådgiver

Appendix C: Questionnaire

1.	Hva er virksomhetens hovedsektor? (kun ett kryss)												
	<table border="0"> <tr> <td><input type="checkbox"/> Tele og data</td> <td><input type="checkbox"/> Media og presse</td> <td><input type="checkbox"/> Politi/redningstjeneste</td> </tr> <tr> <td><input type="checkbox"/> Olje og gass</td> <td><input type="checkbox"/> Transport</td> <td><input type="checkbox"/> Forskning og utdanning</td> </tr> <tr> <td><input type="checkbox"/> Offentlig forvaltning</td> <td><input type="checkbox"/> Bank og finans</td> <td><input type="checkbox"/> Annen sektor</td> </tr> <tr> <td><input type="checkbox"/> Helse og trygd</td> <td><input type="checkbox"/> Kraft og energi</td> <td></td> </tr> </table>	<input type="checkbox"/> Tele og data	<input type="checkbox"/> Media og presse	<input type="checkbox"/> Politi/redningstjeneste	<input type="checkbox"/> Olje og gass	<input type="checkbox"/> Transport	<input type="checkbox"/> Forskning og utdanning	<input type="checkbox"/> Offentlig forvaltning	<input type="checkbox"/> Bank og finans	<input type="checkbox"/> Annen sektor	<input type="checkbox"/> Helse og trygd	<input type="checkbox"/> Kraft og energi	
<input type="checkbox"/> Tele og data	<input type="checkbox"/> Media og presse	<input type="checkbox"/> Politi/redningstjeneste											
<input type="checkbox"/> Olje og gass	<input type="checkbox"/> Transport	<input type="checkbox"/> Forskning og utdanning											
<input type="checkbox"/> Offentlig forvaltning	<input type="checkbox"/> Bank og finans	<input type="checkbox"/> Annen sektor											
<input type="checkbox"/> Helse og trygd	<input type="checkbox"/> Kraft og energi												
2.	Hvor mange ansatte har virksomheten? <input type="checkbox"/> 1-10, <input type="checkbox"/> 11-50, <input type="checkbox"/> 51-200, <input type="checkbox"/> 201-1000, <input type="checkbox"/> over 1000												
3.	Hvilket ledelsessystem/styringssystem for informasjonssikkerhet benyttes? <i>(Ledelsessystem/styringssystem for informasjonssikkerhet: benyttes til å opprette, innføre, drive, overvåke, evaluere, vedlikeholde og forbedre virksomhetens informasjonssikkerhet. Virksomheten får et redskap for å kunne identifisere kritiske verdier og beskytte dem. Formålet med et styringssystem for informasjonssikkerhet er å sikre virksomhetens kontinuitet og redusere eventuell skade ved å forhindre og begrense virkningen av informasjonsmisbruk.)</i> <input type="checkbox"/> Sertifisert iht. BS 7799, NS-ISO/IEC 17799 <input type="checkbox"/> Uformell bruk av BS 7799, NS-ISO/IEC 17799, eller harmonisering mot standarden <input type="checkbox"/> Annet proprietær ledelses- eller styringssystem. Hvilket? _____ <input type="checkbox"/> Benytter egenutviklet ledelses- eller styringssystem. <input type="checkbox"/> Benytter ikke ledelses- eller styringssystem.												
4.	I hvilket år ble første versjon av ledelsessystemet/styringssystemet for informasjonssikkerhet implementert? Årstall: _____												
5.	Alle kan ha et ansvar mht. informasjonssikkerhet i virksomheten, men hvor mange er det totalt som arbeider med oppgaver knyttet til informasjonssikkerhet i virksomheten? <i>(Eksempler på oppgaver knyttet til informasjonssikkerhet: overordnet koordinering, konfigurering og vedlikehold av brannmur, fysisk sikkerhet, personellsikkerhet, kommunikasjonssikkerhet, administrasjon av tilgangskontroll, etc.)</i> Antall årsverk som arbeider med oppgaver knyttet til informasjonssikkerhet: <input type="checkbox"/> 0-1, <input type="checkbox"/> 2-4, <input type="checkbox"/> 5-10, <input type="checkbox"/> 11-20, <input type="checkbox"/> 21-50, <input type="checkbox"/> over 50 Antall personer som utgjør årsverkene: <input type="checkbox"/> 0-1, <input type="checkbox"/> 2-4, <input type="checkbox"/> 5-10, <input type="checkbox"/> 11-20, <input type="checkbox"/> 21-50, <input type="checkbox"/> over 50												
6.	Ref. foregående spørsmål, hvor stor innsats benyttes til forebyggende informasjonssikkerhet? Arbeidet med informasjonssikkerhet kan inndeles i tre faser; forebygge, oppdage og reagere. En del tiltak kan være vanskelig å plassere i kun en av fasene. <i>(Typisk vil fysiske tiltak, tilgangskontroll, antivirus, etc. være forebyggende. Alarmer, IDS, oppsett av logging, etc. vil være tiltak som bidrar til å oppdage sikkerhetsbrudd. Kontinuitetsplaner, team for å håndtere sikkerhetsbrudd, etc. vil typisk være tiltak for å reagere, håndtere og gjenopprette virksomhetskritiske funksjoner etter et sikkerhetsbrudd.)</i> Hvor mye av ressursene, i prosent av foregående spørsmål, medgår til forebyggende informasjonssikkerhet: <input type="checkbox"/> 0-10%, <input type="checkbox"/> 11-20%, <input type="checkbox"/> 21-30%, <input type="checkbox"/> 31-40%, <input type="checkbox"/> 41-50%, <input type="checkbox"/> 51-60%, <input type="checkbox"/> 61-70%, <input type="checkbox"/> 71-80%, <input type="checkbox"/> 81-90%, <input type="checkbox"/> 91-100%,												

7.	Har virksomheten en skriftlig informasjonssikkerhetspolicy? <input type="checkbox"/> Ja, <input type="checkbox"/> Nei
8.	Er informasjonssikkerhetspolicyen revidert i løpet av de siste 12 måneder? <input type="checkbox"/> Ja, <input type="checkbox"/> Nei
9.	Hvilken funksjon(er)/rolle(er) i virksomheten har ansvaret for revisjon av informasjonssikkerhetspolicyen? Skriv ditt svar her:
10.	Eventuelt, hvilken andre funksjon(er)/rolle(er) involveres i revisjonen av informasjonssikkerhetspolicyen? Skriv ditt svar her:
11.	Er det etablert et lederforum for informasjonssikkerhet? <input type="checkbox"/> Ja, <input type="checkbox"/> Nei
12.	I tilfelle ja på foregående spørsmål. Er lederforumets ansvar og oppgaver klart definert? <input type="checkbox"/> Ja, lederforumets ansvar og oppgaver er klart definert <input type="checkbox"/> Ansvar og oppgaver er delvis definert I hvilket årstall ble lederforumet etablert: _____
13.	Har det vært gjennomført noen former for kampanjer eller opplæring for å heve bevisstgjøringsnivået mht. de farer som truer informasjonssikkerheten i virksomheten? <input type="checkbox"/> Ja, det er gjennomført bevisstgjøringskampanjer/opplæring rettet mot alle ansatte samt innleid personell i løpet av de siste 12 måneder . <input type="checkbox"/> Ja, det er gjennomført bevisstgjøringskampanjer/opplæring rettet mot enkelte grupper ansatte eller innleid personell i løpet av de siste 12 måneder . <input type="checkbox"/> Nei ikke i løpet av de siste 12 måneder.
14.	Ref. foregående spørsmål for svaralternativene "Ja". Hvilken former for bevisstgjøring/opplæring har vært gjennomført de siste 12 måneder? Skriv ditt svar her:
15.	Ref. spørsmål 13 for svaralternativet "Nei". Har det vært gjennomført bevisstgjøringskampanjer/opplæring mht. de farer som truer informasjonssikkerheten før siste 12 måneder periode? <input type="checkbox"/> Ja, <input type="checkbox"/> Nei I tilfelle "Ja", kan du angi antall år siden siste bevisstgjøringskampanje/opplæring ble gjennomført? Skriv ditt svar her: ____ år

16.	Gjøres det risiko- og/eller sårbarhetsanalyser av informasjonssikkerheten i virksomheten? <input type="checkbox"/> Ja, <input type="checkbox"/> Nei
17.	Når gjennomføres risiko- og/eller sårbarhetsanalyser i virksomheten? Skriv ditt svar her:
18.	Hvilken metode(r) og/eller verktøy benyttes ifm. risiko- og/eller sårbarhetsanalyser i virksomheten? Skriv ditt svar her:
19.	Hvordan beregnes risikoen? Kan du angi formelen(e) for beregning av risikoen i metoden(e)/verktøyet(ene) som er benyttet? Skriv ditt svar her:
20.	Er det gjennomført analyse(r) mht. hvor mye innsats en eventuell motstander må benytte av ressurser for å kunne gjennomføre et vellykket angrep mot virksomheten? <input type="checkbox"/> Ja, dokumentert i rapport <input type="checkbox"/> Ja, men ikke dokumentert <input type="checkbox"/> Nei
21.	Hvor mye ressurser og kostnader er i snitt benyttet for å gjennomføre en analyse? Estimat mht. medgått tid i form av personelltimer: ____ timer Estimat mht. kostnader: _____ kroner
22.	Er det gjennomført interne målinger på bevisstgjøringsnivået hos de ansatte i forhold til de trusler som er rettet mot informasjonssikkerheten i virksomheten? <input type="checkbox"/> Ja, dokumentert i form av rapport(er) <input type="checkbox"/> Nei
23.	Hvis det er gjennomført måling(er) som nevnt i foregående punkt, hvilket resultat ga målingen(e)? Angir resultatet av målingene en tendens? Skriv ditt svar her:
24.	Kontinuitetsplanlegging: Er det etablert prosesser for å utvikle og vedlikeholde forretningskontinuiteten i virksomheten? <input type="checkbox"/> Ja, for samtlige forretningsmessige aspekter i virksomheten. <input type="checkbox"/> Ja, for de mest kritiske forretningsmessige aspektene i virksomheten. <input type="checkbox"/> Ja, for enkelte av de kritiske forretningsmessige aspektene i virksomheten. <input type="checkbox"/> Nei

25.	<p>Hvilke elementer inngår i kontinuitetsplanleggingen?</p> <p><input type="checkbox"/> Risikoanalyser med angivelse av sannsynlighet og konsekvens for mulige hendelser.</p> <p><input type="checkbox"/> Identifisering og prioritering av kritiske forretningsprosesser.</p> <p><input type="checkbox"/> Oversikt og forståelse av de konsekvensene som eventuelle avbrudd i forretningsprosessene vil medføre.</p> <p><input type="checkbox"/> Mulige forsikringsordninger er vurdert som et ledd i kontinuitetsstrategien.</p> <p><input type="checkbox"/> En dokumentert kontinuitetsstrategi er utarbeidet.</p> <p><input type="checkbox"/> Dokumenterte kontinuitetsplaner, katastrofeplaner, kriseplaner, beredskapsplaner, etc. er utarbeidet iht. vedtatt strategi.</p> <p><input type="checkbox"/> Planene testes ved jevne mellomrom.</p> <p style="padding-left: 40px;">Frekvens på testing er: _____</p> <p style="padding-left: 40px;">Når ble den sist testet: _____</p> <p><input type="checkbox"/> Planene oppdateres ved jevne mellomrom.</p> <p style="padding-left: 40px;">Frekvens på oppdatering er: _____</p> <p><input type="checkbox"/> Ansvar for koordineringen av kontinuitetsprosessen er plassert.</p>
26.	<p>Føres det statistikk mht. antall faktiske brudd og forsøk på brudd på informasjonssikkerheten?</p> <p><input type="checkbox"/> Ja, både faktiske brudd og forsøk på brudd</p> <p><input type="checkbox"/> Ja, kun faktiske brudd</p> <p><input type="checkbox"/> Ja, kun forsøk på brudd</p> <p><input type="checkbox"/> Nei</p>
27.	<p>I tilfelle "Ja" på foregående spørsmål. Hvor mange år tilbake i tid inngår i statistikken?</p> <p>Skriv ditt svar her: _____ år</p>
28.	<p>Ref. de foregående spørsmål, hvilke metode(r)/verktøy etc. benyttes til å registrere forsøk på brudd?</p> <p>Skriv ditt svar her:</p>
29.	<p>Ref. de foregående spørsmålene, hvilke metode(r)/verktøy etc. benyttes for å fange opp og registrere de faktiske sikkerhetsbrudd?</p> <p>Skriv ditt svar her:</p>
30.	<p>Håndtering av sikkerhetsbrudd. Finnes det et team for håndtering av brudd på informasjonssikkerheten i virksomheten?</p> <p><input type="checkbox"/> Ja, teamet er definert, prosedyrer er dokumentert og teamet har øvd på håndteringen av sikkerhetsbrudd</p> <p><input type="checkbox"/> Ja, teamet er definert og prosedyrer er dokumentert.</p> <p><input type="checkbox"/> Ja, teamet er definert.</p> <p><input type="checkbox"/> Nei, et team er foreløpig ikke definert.</p>
31.	<p>I tilfelle "Ja" på foregående spørsmål. Hvor lenge har teamet eksistert? I mindre virksomheter kan det være akseptabelt med kun en person.</p> <p>Skriv ditt svar her: _____ år</p>

32.	<p>Hvilke konsekvenser har blitt påført virksomheten siden 1999?</p> <p><input type="checkbox"/> tap av liv, <input type="checkbox"/> negativ omtale i media, <input type="checkbox"/> tap av markedsandeler, <input type="checkbox"/> følgekonskvenser for samfunnet, <input type="checkbox"/> utilgjengelige systemer og tjenester, <input type="checkbox"/> andre.</p> <p>For alternativ "andre" vennligst beskriv konsekvensene:</p>
33.	<p>Det er ønskelig at konsekvensene beregnes i form av økonomiske tap i form av kroner. Vennligst registrer de faktiske konsekvenser i form av økonomisk tap for de seneste 6 år.</p> <p>2004: <input type="checkbox"/> vet ikke, <input type="checkbox"/> 0 - 9999 kr., <input type="checkbox"/> 10.000 - 99.999 kr., <input type="checkbox"/> 100.000 - 999.999 kr., <input type="checkbox"/> 1,0 - 9,9 mill.kr., <input type="checkbox"/> over 10 mill. kr.</p> <p>2003: <input type="checkbox"/> vet ikke, <input type="checkbox"/> 0 - 9999 kr., <input type="checkbox"/> 10.000 - 99.999 kr., <input type="checkbox"/> 100.000 - 999.999 kr., <input type="checkbox"/> 1,0 - 9,9 mill.kr., <input type="checkbox"/> over 10 mill. kr.</p> <p>2002: <input type="checkbox"/> vet ikke, <input type="checkbox"/> 0 - 9999 kr., <input type="checkbox"/> 10.000 - 99.999 kr., <input type="checkbox"/> 100.000 - 999.999 kr., <input type="checkbox"/> 1,0 - 9,9 mill.kr., <input type="checkbox"/> over 10 mill. kr.</p> <p>2001: <input type="checkbox"/> vet ikke, <input type="checkbox"/> 0 - 9999 kr., <input type="checkbox"/> 10.000 - 99.999 kr., <input type="checkbox"/> 100.000 - 999.999 kr., <input type="checkbox"/> 1,0 - 9,9 mill.kr., <input type="checkbox"/> over 10 mill. kr.</p> <p>2000: <input type="checkbox"/> vet ikke, <input type="checkbox"/> 0 - 9999 kr., <input type="checkbox"/> 10.000 - 99.999 kr., <input type="checkbox"/> 100.000 - 999.999 kr., <input type="checkbox"/> 1,0 - 9,9 mill.kr., <input type="checkbox"/> over 10 mill. kr.</p> <p>1999: <input type="checkbox"/> vet ikke, <input type="checkbox"/> 0 - 9999 kr., <input type="checkbox"/> 10.000 - 99.999 kr., <input type="checkbox"/> 100.000 - 999.999 kr., <input type="checkbox"/> 1,0 - 9,9 mill.kr., <input type="checkbox"/> over 10 mill. kr.</p>
34.	<p>I de tilfeller hvor virksomheten har arbeidet med, og hatt fokus på informasjonssikkerheten i virksomheten over en periode på flere år, finnes det statistikk eller annen dokumentasjon på resultatet av arbeidet?</p> <p><input type="checkbox"/> Ja, <input type="checkbox"/> Nei</p>
35.	<p>Ref. foregående spørsmål, er det mulig for utsteder av spørreundersøkelsen å få tilgang til statistikk/dokumentasjon?</p> <p><input type="checkbox"/> Ja, <input type="checkbox"/> Nei</p> <p>I tilfelle "Ja", vennligst informer undertegnede om at din virksomhet kan stille statistikk/dokumentasjonsunderlag til rådighet. Vi avtaler deretter virksomhetens betingelser og eventuelle behov for anonymisering og "vasking" av dataene før overlevering.</p>

Med vennlig hilsen
Frank-Arne Stamland

frank-arne.stamland@vincit.no

Kontor: 35 57 41 38
Mobil: 90 57 67 57

Appendix D: The answers from the questionnaire

We need to guarantee the anonymity of the participants in the survey and this led to removing of the following answers in the questionnaire: 1, 2, 9, 10, 14 and 21. Question 21 was misunderstood and connected with the questions #16-19 about risk analysis instead of question #20. All the main questions, except from the questions #20-21 about analysis of how much achievement a potential adversary has to use to succeed, are summarized in chapter 4.

	Skjema #1	Skjema #2	Skjema #3	Skjema #4	Skjema #5
3	Sertifisert	Uformell bruk	Sertifisert	Uformell bruk	Sertifisert
4	Før 1990	2002	2002	2003	2003
5a	2-4	21-50	Over 50	Over 50	5-10
5b	5-10	Blank	Over 50	Over 50	Blank
6	21-30%	11-20%	21-30%	51-60%	0-10%
7	Ja	Ja	Ja	Ja	Ja
8	Ja	Ja	Ja	Ja	Ja
11	Ja	Ja	Ja	Ja	Ja
12	Ja, klart definert	Ja, klart definert	Ja, klart definert	Ja, klart definert	Ja, klart definert
12b	2003	Blank	2002	1998	2003
13	Nei	Ja, mot alle	Ja, mot alle	Ja, mot alle	Ja, mot alle
15	Ja	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
15b	2 år	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
16	Ja	Ja	Ja	Ja	Ja
17	Hvert 2.år	Nye prosjekter	Ved større endringer	Nye prosjekter	Hvert år
	Nye systemer	Nye systemer	Periodisk, kritiske områder	Nye systemer	Nye prosjekter
			På bakgrunn av hendelser	Ved større endringer	Nye systemer
				Ved outsourcing og etter planlegging	
18	Risk Assessment	Internversjon/Selvlaget	Internversjon/Selvlaget	Telerisk	Internversjon/Selvlaget
				FRA(forenklet RA)	
				Sjekklistor	
				HASOP	
19	Verktøy	Kostnadsbilde	Trussel x sårbarhet x frekvens	Sannsynlighet x konsekvens	Trusler x sannsynlighet x konsekvens
				Kostnadsbilde	
20	Nei	Nei	Ja, men ikke dokumentert	Ja, dokumentert i rapport	Nei
			Gjelder fysisk sikkerhet	Gjelder fysisk sikkerhet	
22	Nei	Nei	Nei	Ja, dokumentert	Nei
23	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Kunnskapen hos den enkelte er for dårlig	
24	Ja, alt. 2	Ja, alt. 3	Ja, alt. 3	Ja, alt. 2	Ja, alt. 2
25					
25b	Nei	Ja	Ja	Ja	Ja
25c	Ja	Ja	Nei	Ja	Ja
25d	Ja	Nei	Ja	Ja	Ja
25e	Nei	Ja	Nei	Ja	Ja
25f	Nei	Nei	Nei	Ja	Nei
25g	Ja	Nei	Ja	Ja	Ja

	Skjema #1	Skjema #2	Skjema #3	Skjema #4	Skjema #5
25h	Ja	Nei	Ja	Ja	Ja
25i	Halvårlig	Ikke besvart	Ikke besvart	Hvert tredje år	Årlig
25j	4-6 mnd	Ikke besvart	Ikke besvart	7-12 mnd	7-12 mnd
25k	Ja	Nei	Ja	Ja	Ja
25l	Halvårlig	Ikke besvart	Ikke besvart	Halvårlig	Årlig
25m	Nei	Nei	Ja	Ja	Ja
26	Ja, alt. 1	Nei	Ja, alt. 3	Ja, alt. 1	Ja, alt. 1
27	2 år	Ikke besvart	2 år	2 år	1 år
28	Applikasjon på intranett	Ikke besvart	Aksesskontroll, viruskontroll, IDS-logger, Brannmurlogger, OS-logger	Regneark i månedlig rapport	Egen avviksordning, samt logger på IT-avdelingen
29	Applikasjon på intranett	Ikke besvart	Egen applikasjon	IDS, interne kontroll rutiner, målinger (passord)	Egen avviksordning, samt logger på IT-avdelingen
30	Ja, alternativ 3	Ja, alternativ 3	Ja, alt. 1	Ja, alt. 1	Nei
31	1 år	2 år	Mer enn 10 år	4 år	Ikke aktuelt
32	ingen	negativ omtale i media, tap av markedsandeler	negativ omtale i media, utilgjengelige systemer og tjenester, andre; Refusjoner/avkortning av inntekter	negativ omtale i media, utilgjengelige systemer og tjenester	negativ omtale i media, utilgjengelige systemer og tjenester
33	0 - 9999 kr	vet ikke	0 - 9999 kr	100.000 - 999.999 kr	vet ikke
	0 - 9999 kr	vet ikke	100.000 - 999.999 kr	100.000 - 999.999 kr	vet ikke
	0 - 9999 kr	vet ikke	1,0 - 9,9 mill.kr	100.000 - 999.999 kr	vet ikke
	0 - 9999 kr	vet ikke	100.000 - 999.999 kr	100.000 - 999.999 kr	vet ikke
	0 - 9999 kr	vet ikke	vet ikke	100.000 - 999.999 kr	vet ikke
	0 - 9999 kr	vet ikke	vet ikke	100.000 - 999.999 kr	vet ikke
34	Nei	Nei	Ja	Nei	Ja
35	Nei	Nei	Nei	Nei	Ja

	Skjema #6	Skjema #7	Skjema #8	Skjema #9	Skjema #10
3	Uformell bruk	Uformell bruk	Uformell bruk	Egenutviklet	Benytter ikke
4	2000	2001	Blank	1995	Blank
5a	2-4	5-10	0-1	11-20	2-4
5b	5-10	Blank	2-4	5-10	2-4
6	51-60%	Ikke besvart	41-50%	31-40%	81-90%
7	Ja	Ja	Ja	Ja	Ja
8	Nei	Ja	Ja	Nei	Nei
11	Ja	Ja	Ja	Ja	Nei
12	Ja, klart definert	Ja, klart definert	Ja, klart definert	Delvis definert	
12b	2000	2001	1990	1995	
13	Ja, mot alle	Ja, mot enkelte grupper	Ja, mot alle	Ja, mot enkelte grupper	Ja, mot alle
15	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
15b	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
16	Nei	Ja	Ja	Ja	Ja
17		Hvert år	Hvert år	Kontinuerlig	Hvert år
					Når trusselbildet endres
18		Internversjon/ Selvlaget Ekstern hjelp	Internversjon/ Selvlaget	Internversjon/ Selvlaget	DSB veileder i ROS analyse

	Skjema #6	Skjema #7	Skjema #8	Skjema #9	Skjema #10
19		Ikke forstått	Ikke besvart	Risikokostnad = Frekvens x skadekostnad	Sannsynlighet x konsekvens
20	Nei	Nei	Ja, men ikke dokumentert	Nei	Nei
22	Nei	Nei	Nei	Nei	Nei
23					
24	Ja, alt. 2	Ja, alt. 2	Ja, alt. 1	Ja, alt. 2	Ja, alt. 2
25					
25b	Nei	Ja	Ja	Ja	Ja
25c	Ja	Nei	Ja	Ja	Ja
25d	Nei	Nei	Ja	Ja	Ja
25e	Nei	Nei	Nei	Nei	Nei
25f	Nei	Nei	Ja	Ja	Nei
25g	Ja	Ja	Ja	Ja	Ja
25h	Nei	Ja	Nei	Ja	Ja
25i	Ikke besvart	Ikke besvart	Ikke besvart	Årlig	Årlig
25j	Ikke besvart	Ikke besvart	Ikke besvart	4-6 mnd	7-12 mnd
25k	Ja	Ja	Ja	Ja	Ja
25l	Ikke besvart	Ikke besvart	Årlig	Årlig	Årlig
25m	Ja	Ja	Ja	Ja	Ja
26	Nei	Ja, alt. 1	Ja, alt. 1	Ja, alt. 2	Ja, alt. 1
27	Ikke besvart	4 år	3 år	3 år	4 år
28		Loggverktøyer	Logger knyttet mot programvaren. Kan endres over tid.	Rapportering	IDS
29		Avviksrutiner (egen prosedyre som skal fylles ut og sendes til sikkerhetsrådgiver)	Logg, se 28	Rapportering	IDS og Internkontrollsystem
30	Ja, alt. 1	Ja, alt. 1	Ja, alt. 2	Ja, alt. 2	Ja, alt. 3
31	4 år	3 år	1 år	4 år	2 år
32	utilgjengelige systemer og tjenester	ingen		negativ omtale i media, utilgjengelige systemer og tjenester	utilgjengelige systemer og tjenester
33	10.000 - 99.999 kr	0 - 9999 kr	vet ikke	10.000 - 99.999 kr	10.000 - 99.999 kr
	10.000 - 99.999 kr	0 - 9999 kr	vet ikke	100.000 - 999.999 kr	10.000 - 99.999 kr
	10.000 - 99.999 kr	0 - 9999 kr	vet ikke	100.000 - 999.999 kr	vet ikke
	10.000 - 99.999 kr	0 - 9999 kr	vet ikke	vet ikke	vet ikke
	10.000 - 99.999 kr	0 - 9999 kr	vet ikke	vet ikke	vet ikke
	10.000 - 99.999 kr	0 - 9999 kr	vet ikke	vet ikke	vet ikke
34	Nei	Ja	Ja	Ja	Nei
35	Nei	Nei	Nei	Nei	Nei

	Skjema #11	Skjema #12	Skjema #13	Skjema #14	Skjema #15
3	Uformell bruk	Uformell bruk	Benytter ikke	Uformell bruk	Uformell bruk
4	2000	1999	Blank	2000	2000
5a	Over 50	21-50	2-4	5-10	2-4
5b	Over 50	Over 50	Blank	5-10	11-20
6	41-50%	71-80%	21-30%	41-50%	61-70%
7	Ja	Ja	Ja	Ja	Ja

	Skjema #11	Skjema #12	Skjema #13	Skjema #14	Skjema #15
8	Ja	Nei	Ja	Nei	Ja
11	Ja	Nei	Nei	Nei	Nei
12	Ja, klart definert				
12b	2000				
13	Ja, mot alle	Ja, mot enkelte grupper	Ja, mot alle ansatte	Nei	Ja, mot alle
15	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	Ja	Ikke aktuelt
15b	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	2 år	Ikke aktuelt
16	Ja	Ja	Ja	Ja	Ja
17	Hvert 2.år	Ved revisjon og kontroll	Nye prosjekter	Nye systemer	Nye prosjekter
			Nye systemer	Ved større endringer	Nye systemer
			Kontinuerlig		Ved større endringer
18	CRAMM	Internversjon/ Selvlaget ISF: SARA og SPRINT	Kartlegging av sårbarheter og kritiske faktorer	SBA	Internversjon/ Selvlaget
19	Trusler x sårbarhet x verdier	Eisenhower Matrix	Sårbarheter og kritiske faktorer	SBA	Ikke besvart
20	Ja, men ikke dokumentert	Ja, men ikke dokumentert	Nei	Nei	Nei
22	Nei	Nei	Nei	Nei	Nei
23					
24	Ja, alt. 2	Ja, alt. 1	Ja, alt. 3	Ja, alt. 2	Nei
25					
25b	Ja	Ja	Ja	Ja	Nei
25c	Ja	Ja	Nei	Ja	Nei
25d	Ja	Ja	Ja	Nei	Nei
25e	Nei	Nei	Nei	Nei	Nei
25f	Ja	Ja	Nei	Nei	Nei
25g	Ja	Ja	Nei	Nei	Nei
25h	Nei	Ja	Nei	Nei	Nei
25i	Ikke besvart	Årlig	Ikke besvart	Ikke besvart	Ikke besvart
25j	Ikke besvart	4-6 mnd	Ikke besvart	Ikke besvart	Ikke besvart
25k	Ja	Ja	Ja	Nei	Nei
25l	Hvert annet år	Årlig	Etter behov	Ikke besvart	Ikke besvart
25m	Ja	Ja	Ja	Nei	Nei
26	Nei	Ja, alt. 1	Nei	Ja, alt. 2	Nei
27	Ikke besvart	4 år	Ikke besvart	2 år	Ikke besvart
28	IDS, FW, manuell nettverksovervåking , nettverksanalyse	Egenutviklet system		IDS rapporter, Gjennomgang av FW-logger	Sjekk av div logger, IDS
29	IDS, FW, manuell nettverksovervåking , nettverksanalyse	Egenutviklet system	Gjennomgang av logger samt innrapportering om brudd.	Innrapportering	
30	Ja, alt. 1	Ja, alt. 2	Ja, alt. 3	Ja, alt. 1	Ja, alt. 3
31	4 år	Ikke besvart	2 år	4 år	2 år
32	Ingen	negativ omtale i media, følgekonsekvenser for samfunnet, utilgjengelige systemer og tjenester	utilgjengelige systemer og tjenester	utilgjengelige systemer og tjenester	
33	0 - 9999 kr	over 10 mill	0 - 9999 kr	10.000 - 99.999 kr	vet ikke

	Skjema #11	Skjema #12	Skjema #13	Skjema #14	Skjema #15
	0 - 9999 kr	over 10 mill	0 - 9999 kr	vet ikke	vet ikke
	0 - 9999 kr	over 10 mill	10.000 - 99.999 kr	vet ikke	vet ikke
	0 - 9999 kr	over 10 mill	vet ikke	vet ikke	vet ikke
	0 - 9999 kr	over 10 mill	vet ikke	vet ikke	vet ikke
	0 - 9999 kr	over 10 mill	vet ikke	vet ikke	vet ikke
34	Nei	Ja	Ja	Nei	Nei
35	Nei	Nei	Nei	Nei	Nei

	Skjema #16	Skjema #17	Skjema #18	Skjema #19	Skjema #20
3	Sertifisert	Uformell bruk	Benytter ikke	Uformell bruk	Uformell bruk
4	1994	2001	Blank	2004	2004
5a	21-50	Over 50	5-10	2-4	5-10
5b	Blank	Over 50	5-10	Blank	5-10
6	Ikke besvart	31-40%	71-80%	31-40%	Ikke besvart
7	Ja	Ja	Nei	Ja	Ja
8	Ja	Ja	Nei	Ja	Ja
11	Nei	Nei	Nei	Ja	Nei
12				Delvis definert	
12b				2004	
13	Ja, mot alle	Ja, mot alle	Nei	Nei	Ja, mot enkelte grupper
15	Ikke aktuelt	Ikke aktuelt	Nei	Nei	Ikke aktuelt
15b	Ikke aktuelt	Ikke aktuelt	Ikke besvart	Ikke besvart	Ikke aktuelt
16	Ja	Ja	Nei	Ja	Ja
17	Hvert år	Hvert år		Hvert år	Hvert 2.år
		Ved større endringer			Kontinuerlig
		Nye prosjekter			
18	Internversjon/ Selvlaget	NS/ISO 5814		ROS-analyse	NS 17799, Ekstern hjelp
19	Ikke besvart	Kvalitativt og kvantitativt		Sannsynlighet x konsekvens	Sannsynlighetsvurdering
20	Nei	Nei	Nei	Nei	Nei
22	Ja, dokumentert	Nei	Nei	Nei	Nei
23					
24	Ja, alt. 1	Ja, alt. 2	Ja, alt. 2	Ja, alt. 3	Ja, alt. 1
25					
25b	Nei	Ja	Nei	Ja	Ja
25c	Nei	Ja	Ja	Ja	Ja
25d	Nei	Nei	Ja	Nei	Ja
25e	Nei	Nei	Nei	Nei	Nei
25f	Nei	Ja	Ja	Nei	Nei
25g	Nei	Ja	Ja	Ja	Ja
25h	Nei	Ja	Nei	Ja	Ja
25i	Ikke besvart	Årlig	Ikke besvart	Halvårlig	Hvert annet år
25j	Ikke besvart	7-12 mnd	Ikke besvart	1-3 mnd	1-2 år
25k	Nei	Ja	Ja	Ja	Nei
25l	Ikke besvart	Etter behov	Ikke besvart	Halvårlig	Ikke besvart
25m	Nei	Ja	Ja	Ja	Ja
26	Ja, alt. 2	Ja, alt. 1	Nei	Nei	Ja, alt. 1
27	Ikke besvart	Ikke besvart	Ikke besvart	Ikke besvart	3 år

	Skjema #16	Skjema #17	Skjema #18	Skjema #19	Skjema #20
28		Intern rapportering, IDS, nettverksovervåking	Brannmur, IDS-system, Antivirus system		Firewall mgmt m/diverse verktøy for antivirus
29		Intern rapportering, IDS, nettverksovervåking	Brannmur, IDS-system, Antivirus system		Automatisk registrering etter FW, IDS system er under vurdering
30	Ja, alt. 1	Ja, alt. 2	Nei	Nei	Nei
31	Ikke besvart	Ikke besvart	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
32		negativ omtale i media	utilgjengelige systemer og tjenester	følgekonsekvenser for samfunnet, utilgjengelige systemer og tjenester, andre	Ingen
32b					
33	vet ikke	vet ikke	vet ikke	vet ikke	0 - 9999 kr
	vet ikke	vet ikke	100.000 - 999.999 kr	vet ikke	0 - 9999 kr
	vet ikke	vet ikke	1,0 - 9,9 mill.kr	vet ikke	0 - 9999 kr
	vet ikke	vet ikke	vet ikke	vet ikke	0 - 9999 kr
	vet ikke	vet ikke	vet ikke	vet ikke	0 - 9999 kr
	vet ikke	vet ikke	vet ikke	vet ikke	0 - 9999 kr
34	Nei	Ja	Nei	Nei	Ja
35	Nei	Nei	Nei	Nei	Nei

	Skjema #21	Skjema #22	Skjema #23	Skjema #24	Skjema #25
3	Uformell bruk	Benytter ikke	Benytter ikke	Uformell bruk	Sertifisert
4	2001	Blank	Blank	2003	2001
5a	0-1	0-1	2-4	2-4	0-1
5b	2-4	Blank	5-10	2-4	2-4
6	81-90%	0-10%	41-50%	11-20%	21-30%
7	Ja	Nei	Nei	Ja	Ja
8	Nei	Nei	Nei	Ja	Nei
11	Ja	Nei	Nei	Nei	Ja
12	Ja, klart definert				Ja, klart definert
					2001
13	Nei	Nei	Nei	Ja, mot alle	Ja, mot enkelte grupper
15	Nei	Nei	Ja	Ikke aktuelt	Ja
15b	Ikke besvart	Ikke aktuelt	2 år	Ikke aktuelt	1 år
16	Ja	Nei	Nei	Ja	Ja
17	Nå for første gang			Ved større endringer	Ved sertifisering
				Hvert år	
18	Ikke besvart	Ikke besvart	Ikke besvart	Internversjon/Selvlaget	NS 17799
				Datatilsynets	
19	Ikke besvart	Ikke besvart	Ikke besvart	Ikke besvart	Ikke besvart
20	Nei	Nei	Nei	Ja, dokumentert i rapport	Ja, dokumentert i rapport
22	Nei	Nei	Nei	Nei	Ja, dokumentert i rapport
23					BS 7799 er omfattende. En tendens er at IS må informeres ofte og i en kontekst de ansatte forstår (for

	Skjema #21	Skjema #22	Skjema #23	Skjema #24	Skjema #25
					eksempel bruk av email)
24	Ja, alt. 3	Ja, alt. 1	Ja, alt. 2	Ja, alt. 2	Ja, alt. 2
25					
25b	Nei	Nei	Nei	Nei	Ja
25c	Ja	Nei	Ja	Ja	Ja
25d	Nei	Nei	Ja	Ja	Ja
25e	Nei	Ja	Nei	Ja	Ja
25f	Nei	Nei	Nei	Ja	Ja
25g	Nei	Nei	Nei	Ja	Ja
25h	Nei	Nei	Nei	Nei	Nei
25i	Ikke besvart	Ikke besvart	Ikke besvart	Ikke besvart	Ikke besvart
25j	Ikke besvart	Ikke besvart	Ikke besvart	Ikke besvart	Ikke besvart
25k	Nei	Nei	Nei	Ja	Nei
25l	Ikke besvart	Ikke besvart	Ikke besvart	Årlig	Ikke besvart
25m	Nei	Nei	Nei	Ja	Ja
26	Nei	Nei	Nei	Ja, alt. 1	Ja, alt. 1
27	Ikke besvart	Ikke besvart	Ikke besvart	1 år	4 år
28					Manuelt hos Admin, Help Desk software hos IT
29				ODS, FW, Logganalyse	Manuelt hos Admin, Help Desk software hos IT
30	Nei	Nei	Nei	Ja, alt. 1	Ja, alt. 1
31	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt	1 år	4 år
32	ingen		utilgjengelige systemer og tjenester	utilgjengelige systemer og tjenester, andre	
32b					
33	0 - 9999 kr	vet ikke	vet ikke	10.000 - 99.999 kr	vet ikke
	0 - 9999 kr	vet ikke	vet ikke	100.000 - 999.999 kr	vet ikke
	0 - 9999 kr	vet ikke	vet ikke	vet ikke	vet ikke
	0 - 9999 kr	vet ikke	vet ikke	vet ikke	vet ikke
	0 - 9999 kr	vet ikke	vet ikke	vet ikke	vet ikke
	0 - 9999 kr	vet ikke	vet ikke	vet ikke	vet ikke
34	Nei	Nei	Nei	Nei	Nei
35	Nei	Nei	Nei	Nei	Nei

	Skjema #26	Skjema #27	Skjema #28
3	Sertifisert	Uformell bruk	Benytter ikke
4	2001	2002	Blank
5a	5-10	5-10	5-10
5b	Blank	Blank	Blank
6	11-20%	31-40%	41-50%
7	Ja	Ja	Nei
8	Ja	Ja	Nei
11	Ja	Nei	Nei
12	Ja, klart definert		
13	Ja, mot enkelte grupper	Ja, mot alle	Ja, mot enkelte grupper
15	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt
15b	Ikke aktuelt	Ikke aktuelt	Ikke aktuelt

	Skjema #26	Skjema #27	Skjema #28
16	Ja	Ja	Ja
17	Ved større endringer	Hvert år	Ikke besvart
18	Ekstern hjelp	Ekstern hjelp	Ikke besvart
	ROS-analyse		
	Telerisk		
19	Ikke besvart	Ikke besvart	Ikke besvart
20	Nei	Nei	Nei
22	Ja, dokumentert i rapport	Nei	Nei
23			
24	Ja, alt. 2	Ja, alt. 2	Nei
25			
25b	Ja	Ja	Nei
25c	Nei	Nei	Nei
25d	Ja	Ja	Nei
25e	Nei	Nei	Nei
25f	Nei	Ja	Nei
25g	Ja	Ja	Nei
25h	Ja	Ja	Nei
25i	Årlig	Årlig	Ikke besvart
25j	Ikke besvart	7-12 mnd	Ikke besvart
25k	Nei	Ja	Nei
25l	Ikke besvart	Årlig	Ikke besvart
25m	Nei	Ja	Nei
26	Ja, alt. 1	Ja, alt. 2	Nei
27	3 år	2 år	Ikke besvart
28			Ikke besvart
29	Hendelses-rapporteringsrutine r med premiering		
30	Ja, alt. 3	Ja, alt. 1	Nei
31	3 år	2 år	Ikke besvart
32		negativ omtale i media, følgekonsvenser for samfunnet, utilgjengelige systemer og tjenester	utilgjengelige systemer og tjenester
32b			
33	vet ikke	vet ikke	vet ikke
	vet ikke	vet ikke	vet ikke
	vet ikke	vet ikke	vet ikke
	vet ikke	vet ikke	vet ikke
	vet ikke	vet ikke	vet ikke
	vet ikke	vet ikke	vet ikke
34	Ja	Nei	Nei
35	Nei	Nei	Nei

Appendix E: The questionnaire translated into English with an explanation and intentions

This appendix covers an explanation of the questions and the intention with the questions in the questionnaire. The questionnaire was originally written in Norwegian and distributed to organisations in Norway. The Norwegian version has precedence versus the following version in English.

Appendix A, contains the originally version of the questionnaire.

Question #1: What is the main activity in the organisation?

The alternatives are as follows:

- Telecommunication and IT
- Oil and gas
- Public administration
- Health and social security
- Media and press
- Transport/communication
- Banking and finance
- Energy
- Police and rescue service
- Research and education
- Others

Input to thesis: Makes it possible to sort the answers regarding the main activity or business sector.

The alternatives were selected from a scheme for reporting security breaches in Norway [8]. The scheme is developed by the Centre for Information Security (SIS) [8] in Norway (“Rapport om IT-sikkerhetshendelse”).

Question #2: How many employees within the organisation? The alternatives regarding the answer are the following: 1-10, 11-50, 51-200, 201-1000 and above 1000.

Input to thesis: We need to know how large the organisations are. It also makes it possible to analyse whether there is any correlation between the maturity of the ISMS and the number of employees.

Question #3: What kind of ISMS is in use?

The alternatives are:

- Certified according to BS 7799, NS-ISO/IEC 17799
- Informal use of BS 7799, NS-ISO/IEC 17799, or harmonisation towards the standard
- Other ISMS. What?
- Make use of own developed ISMS
- Do not make use of any ISMS.

Input to thesis: We will get information about which ISMS is implemented in the organisations. “Certified organisation” will result in maturity level 3 and above. No use of ISMS will probably indicate maturity level 1 as a maximum. Is there a trend regarding the use of other ISMS? The organisations which use other ISMS are asked to answer which one is in use. Does BS 7799 have any competitors?

Question #4: When was the first version of the ISMS implemented? Year: _____

- Input to thesis: Is there any reduction in the consequences from the year of implementation and forward? There are many aspects which have to be taken into consideration. In the last years there has for example been a heavy increase in the number of security breaches.
- Question #5: All employees may have responsibilities regarding IS, but how many work actively with IS in the organisation? It was possible to mark the following range of checkboxes.
The number of jobs attached to IS activities, converted to man-labour years:
☐ 0-1, ☐ 2-4, ☐ 5-10, ☐ 11-20, ☐ 21-50, ☐ above 50
The number of employees who perform these man-labour years:
☐ 0-1, ☐ 2-4, ☐ 5-10, ☐ 11-20, ☐ 21-50, ☐ above 50
- Input to thesis: An indication regarding how many resources are used on IS compared to the number of employees. Resources used on IS will, of course, depend on the kind of business.
- Question #6: Referring to the previous question, how much effort is used on preventive measures? Hint: A rough classification of protective measures distinguishes between: prevention, detection and reaction. Some measures may be difficult to place in only one category.

How much of the IS resource in the previous question is used on preventive measures? Please report the answer in the following percent categories:
☐ 0-10%, ☐ 11-20%, ☐ 21-30%, ☐ 31-40%, ☐ 41-50%, ☐ 51-60%, ☐ 61-70%,
☐ 71-80%, ☐ 81-90%, ☐ 91-100%
- Input to thesis: Too little effort used on preventative measures may indicate that the limited number of IS personnel only manage to handle troubleshooting.
- Question #7: Does the organisation have a written IS policy?
☐ Yes, ☐ No
- Input to thesis: Yes, indicates maturity level 2 and above.
No, indicates maturity level 1 and below.
- Question #8: Has the IS policy been revised during the last 12 months?
☐ Yes, ☐ No
- Input to thesis: Yes, indicates maturity level 3 and above.
No: indicates maturity level 2 and below.
- Question #9: Which position(s) in the organisation has the responsibility for performing the audit of the IS-policy?
Write your answer here:
- Input to thesis: The answer to the question indicated whether the responsibility is clearly defined.
- Question #10: Are there any other positions are involved in the IS policy audit?
Write your answer here:
- Input to thesis: The number of positions and roles involved in the review of the IS-policy gives us information about how extensive the review process actually is.

- Question #11: Is an IS-management forum established?
☐ Yes, ☐ No
- Input to thesis: A management forum should be established to ensure that there is clear direction and visible management support for security initiatives. Yes, indicates maturity level 3 and above. No: indicates maturity level 2 and below.
- Question #12: In the case of “yes” regarding the preceding question. Is the IS management forum’s responsibility and tasks clearly defined?
☐ Yes, the IS management forum’s responsibility and tasks are clearly defined.
☐ Responsibility and tasks are partly defined.
In which year was the IS management forum established?_____
- Input to thesis: An IS management forum which is partly defined indicates maturity level between level 2 and 3. Responsibility and tasks are not clearly defined.
- Question #13: Have any campaigns or training been performed to raise the level of awareness, regarding the risks that threaten the security of the organisation?
☐ Yes, campaigns/ training directed to all employees and hired personnel were performed during the last 12 months.
☐ Yes, campaigns/ training directed to some groups of employees or hired personnel during the last 12 months.
☐ No not during the last 12 months.
- Input to thesis: Alternative 1: indicates maturity level 4 or 5.
Alternative 2: indicates maturity level 2 or 3.
Alternative 3: indicates maturity level 0 or 1.
- Question #14: Referring to the previous question for alternative “Yes”. What kind of campaigns or training has been performed during the last 12 months?
Write your answer here:
- Input to thesis: The follow-up question will make it possible to more precisely determine the overall maturity level.
- Question #15: Referring to question 13, alternative “No”. Have campaigns/training regarding the risks that threaten the security of the organisation, been performed prior to the last 12 months?
☐ Yes, ☐ No
In the case of Yes”, will it be possible to state the number of years since last campaigns/training program was performed?
Write your answer here:_____ years
- Input to thesis: The answer to the question determines whether campaigns/training is an issue at all in the organisation. More than 3 years since last campaigns/training is equal to “no issue at all”.
- Question #16: Is IS risk analysis performed?
☐ Yes, ☐ No
- Input to thesis: Alternative “Yes” , indicates maturity level 1 to 5.
Alternative “No” , indicates maturity level 0.
- Question #17: When is IS risk analysis performed?
Write your answer here:

Input to thesis: According to the BS 7799-2 certification scheme in Norway IS risk analysis must at least be carried out once a year. Further, IS risk analysis shall be an integrated process in the day to day operation and shall be executed, for example when new services or systems are introduced, and in all other cases where an IS risk analysis will contribute to secure the assets of the organisations.

Question #18: What kind of methods and/or tools are used to perform IS risk analysis?
Write your answer here:

Input to thesis: An introduction to the next question. If a specific tool is used, then we will be able to get information about the formula that is used to calculate the risk.

Question #19: How is the risk calculated? Will it be possible to state the formula which is used to calculate the risk in the method/tool?
Write your answer here:

Input to thesis: A traditional risk analysis where the risk is calculated by probability and consequence may not be sufficient when talking about intelligent attackers. It may be necessary to take threats and vulnerability into consideration. An inventory of the organisation's assets must be in place. A threat exploits vulnerabilities and leads to consequences for the organisation. The organisations assets are destroyed or made unavailable.

The calculation of risk will influence on the estimation of the ISMS maturity.

Question #20: Has any analysis been performed regarding how much effort a potential adversary has to make in order to succeed in an attack?
☐ Yes, documented in a report
☐ Yes, but not documented in a report
☐ No

Input to thesis: Question #20 was misunderstood by many organisations. The answers to the questions are related to the previous question #19 about risk analysis. The answers to this question are rejected and are not an issue in the interpretation of the answers.

Question #21: What are the average costs and the number of resources used to perform this kind of analysis? Resources: measured in man-hours.
Estimate regarding man-hours: _____
Estimate regarding costs: _____ NOK

Input to thesis: As question #20.

Question #22: Have any internal measurements been performed regarding the level of awareness of the staff in relation to the security threats directed towards the IS of the organisation?
☐ Yes, documented in a report
☐ No

Input to thesis: A measurement of the level of awareness will give the organisation an excellent indication whether the organisation is on the right track or if it is in the reverse mode. The "check" and "act" phase of the BS 7799 cycle are important conditions for estimating the ISMS maturity to a "high" level.

Question #23: If measurements have been performed, as mention in the previous question, what are the results of the measurements? Do the results indicate any trend?
Write your answer here:

Input to thesis: The results of the measurements will be very valuable regarding the ISMS maturity estimation. What is the trend?

Question #24: Business continuity management
Are processes for the development and maintenance of the business continuity management established?
☐ Yes, for all commercial aspects in the organisation.
☐ Yes, for the most critical commercial aspects in the organisation.
☐ Yes, for some of the critical commercial aspects in the organisation.
☐ No

Input to thesis: The answer to this question indicates how extensive the business continuity management process is anchored in the organisation.

Question #25: Which elements are a part of the business continuity management process?

☐ Risk analysis, including the likelihood and the impact of possible security incidents (b).
☐ Identification and prioritisation of critical business processes (c).
☐ An overview and understanding of the impact that interruptions are likely to have on the business (d).
☐ Possible insurance schemes are considered as a part of the strategy (e).
☐ A documented business continuity strategy is worked out (f).
☐ Business continuity plans, disaster recovery plans and crisis management plans are worked out according to an approved strategy (g).
☐ The plans are tested at regular intervals (h).
 The testing frequency is: _____ (i)
 When was the plans last tested: _____ (j)
☐ The plans are updated at regular intervals (k)
 The frequency of the updating are: _____ (l)
☐ The responsibility for co-ordinating the business continuity management process is assigned (m).

Input to thesis: The business continuity management process is important regarding the maturity of the ISMS. All checkboxes must be marked to achieve maturity level 5. And in addition, the testing and updating frequency must be at least once a year. The maturity level 4 and below are not specified.

Question #26: Are actual security breaches and attempted security breaches registered in a statistical register?
☐ Yes, both actual breaches and attempts
☐ Yes, only actual breaches
☐ Yes, only attempt on breaches
☐ No

- Input to thesis: An organisation which has a mature ISMS implies control regarding actual security breaches and attempted security breaches. A perfect result from the survey would be as follows. Sufficient organisations have control regarding actual security breaches and they are able to detect attempt on security breaches. Further, they are able to maintain continuous statistical records. If this is the situation it will be possible to compare the kind of ISMS, the year when the ISMS was implemented and the statistical records regarding security breaches.
- Question #27: In the case of "Yes" in the previous question. How far back in time do the statistics exist?
Write your answer here: ____ years
- Input to thesis: The follow-up question will make it possible to determine the overall maturity level more precisely.
- Question #28: With reference to the previous questions. What kind of methods and tools are in use regarding the registration of attempted security breaches?
Write your answer here: ____
- Input to thesis: The follow-up question will make it possible to determine the overall maturity level more precisely.
- Question #29: With reference to the previous questions. What kind of methods and tools are in use regarding the registration of actual security breaches? (successful)
Write your answer here: ____
- Input to thesis: The follow-up question will make it possible to determine the overall maturity level more precisely.
- Question #30: Handling security breaches. Does a team exist in the organisation for handling information security breaches?
☐ Yes, the team has been defined, procedures are documented and the team has practice in the handling of security breaches.
☐ Yes, the team has been defined and procedures are documented.
☐ Yes, the team has been defined.
☐ No, a team has so far not been defined.
- Input to thesis: BS 7799, chapter 8.1.3 [13]: "*Incident management responsibilities and procedures should be established to ensure a quick, effective and orderly response to security incidents.*"
Whether an incident response team exists or not will have an influence on the ISMS maturity level.
- Question #31: In the case of "Yes" in the previous question. How long has the team existed? In smaller organisations it may be acceptable with just one person in the team.
Write your answer here: ____ years
- Input to thesis: The follow-up question will make it possible to determine the overall maturity level more precisely.

Question #32: What kind of consequences has hit the organisation since 1999?

☐ loss of live, ☐ negative publicity in the media, ☐ loss of market shares, ☐ secondary actions with consequences for society, ☐ systems and services not available, ☐ others.

In the case of alternative "others", please describe the consequences:

Input to thesis:

What are the most general consequences that has hit the organisations for the last years? Does the organisation have sufficient control regarding consequences? Control regarding consequences is a part of, e.g., the risk analysis process and the business continuity management process. What kind of consequences that hit the organisation will also be of vital input in regard to which kind of counter-measures should be implemented. In addition, this kind of information is important in justifying necessary funding and the IS-risk the organisation has to deal with.

Question #33: It is desirable to estimate the consequences as financial loss in NOK. Please, register the actual consequences as financial loss for the last 6 years.

2004: ☐ don't know, ☐ 0 - 9999 NOK, ☐ 10.000 - 99.999 NOK, ☐ 100.000 - 999.999 NOK, ☐ 1,0 - 9,9 million NOK, ☐ more than 10 million NOK.

2003: ☐ don't know, ☐ 0 - 9999 NOK, ☐ 10.000 - 99.999 NOK, ☐ 100.000 - 999.999 NOK, ☐ 1,0 - 9,9 million NOK, ☐ more than 10 million NOK.

2002: ☐ don't know, ☐ 0 - 9999 NOK, ☐ 10.000 - 99.999 NOK, ☐ 100.000 - 999.999 NOK, ☐ 1,0 - 9,9 million NOK, ☐ more than 10 million NOK.

2001: ☐ don't know, ☐ 0 - 9999 NOK, ☐ 10.000 - 99.999 NOK, ☐ 100.000 - 999.999 NOK, ☐ 1,0 - 9,9 million NOK, ☐ more than 10 million NOK.

2000: ☐ don't know, ☐ 0 - 9999 NOK, ☐ 10.000 - 99.999 NOK, ☐ 100.000 - 999.999 NOK, ☐ 1,0 - 9,9 million NOK, ☐ more than 10 million NOK.

1999: ☐ don't know, ☐ 0 - 9999 NOK, ☐ 10.000 - 99.999 NOK, ☐ 100.000 - 999.999 NOK, ☐ 1,0 - 9,9 million NOK, ☐ more than 10 million NOK.

Input to thesis:

If the organisations have a good overview of applied consequences for the last years, then we can assume that the maturity of the ISMS is high.

An important issue of the thesis is to inquire whether there is any correlation between consequences and the type of ISMS. When organisations start to implement ISMS, the rate regarding the number of consequences they are aware of may rise in the first years to come. This is because they get improved procedures, a higher level of understanding IS risks, increased awareness regarding IS, and so on. When the ISMS has been present for some years we have to expect fewer incidents that lead to consequences for the organisation. We also want to find out whether it matters to be certified according to BS 7799 versus just harmonising the ISMS with BS 7799.

Four of the respondents have marked "none" for question 32 regarding consequences, but they have not marked question 33. Those 4 questionnaires have been adjusted to 0 - 9999 NOK in annual loss.

Question #34: In those cases where the organisation has worked and focused on IS for a period of several years, do statistics or other documentation exist regarding the results of the work?
☐ Yes, ☐ No

Input to thesis: Security metrics on the effects of the IS work for the last years indicates a very mature ISMS.

Question #35: With reference to the previous question. Is it possible for the issuer of this questionnaire to get access to this statistics/documentation?
☐ Yes, ☐ No

In the case of "Yes", please inform the issuer that your organisation can place statistics/documentation at their disposal. Then we can enter into an agreement about the organisations requirements and also the need for washing the data before the handover.

Input to thesis: A dream world scenario for an IS master student researching the effects of implementing ISMS may be to get full access to statistics and documentation in a range of organisations for a period over several years. One question is, to what degree does this kind of statistics exist? In addition it is, of course, also a challenge for the organisations to hand over this kind of information.

Access to a range of statistics and documentation in an organisation which has worked and focused on IS for a period of several years can be compared with official statistics in order to check the effects of implementing ISMS.

Appendix F: Bootstrap program and the program results

This appendix consists of the R program and 3 program results; certified, informal use of the standard and organisations that do not use any standard.

The “R” program

```
#####
##
## Using bootstrap for calculating the variance for a dataset
##
#####
boot <- function(boot)
{
# Setting the data
cert <- c(2,3,3,2,2,2)
uform <- c(1,3,2,1,1,1,2,1,1,2,2,1,1,1,2)
ubruk <- c(1,1,0,0,0,0)
# Making the tables
certtab <- array(0,dim=c(boot))
uformtab <- array(0,dim=c(boot))
ubruktab <- array(0,dim=c(boot))
# Make the bootstrap samples
for (i in 1:boot)
{
  mval <- 0
# Make bootstrap values for cert table
  for (il in 1:6)
    mval <- mval + sample(cert,1,replace=TRUE)
  certtab[i] <- mval / 6
  mval <- 0
# Make bootstrap values for uform table
  for (il in 1:15)
    mval <- mval + sample(uform,1,replace=TRUE)
  uformtab[i] <- mval / 15
  mval <- 0
# Make bootstrap values for ubruk table
  for (il in 1:6)
    mval <- mval + sample(ubruk,1,replace=TRUE)
  ubruktab[i] <- mval / 6
}
# Sorting the tables to easy get the 5%-95% values
certtab <- sort(certtab)
uformtab <- sort(uformtab)
ubruktab <- sort(ubruktab)
}
#
##### EOF #####
```

Program result “certified”

```
> plot(certtab, type="l")
> certtab[12]
[4] 2
> certtab [950]
[4] 2.66666
> mean(certtab)
```


[4] 2.332167

Program result “informal”

```
> plot(uformtab, type="l")
```

```
> uformtab[12]
```

[4] 1.2

```
> uformtab [950]
```

[4] 1.733333

```
> mean(uformtab)
```

[4] 1.458867

Program result “not using any standard”

```
> plot(ubruktab, type="l")
```

```
> ubruktab[12]
```

[4] 0

```
> ubruktab [950]
```

[4] 0.666667

```
> mean(ubruktab)
```

[4] 0.3375

“R” command for boxplot

```
> boxplot(certtab, uformtab, ubrukttab, main="BoxPlot for the Maturity Level Estimates",  
ylab="Matur:
```